Doctoral theses at NTNU, 2018:46

Vasileios Gkioulos

Securing Tactical Service Oriented Architectures

ISBN 978-82-326-2884-1 (printed version)
ISBN 978-82-326-2885-8 (electronic version)
ISSN 1503-8181

Doctoral Thesis
Vasileios Gkioulos

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Information Security and Communication
Technology

NTNU
Norwegian University of
Science and Technology

Doctoral theses at NTNU, 2018:46

NTNU

NTNU
Norwegian University of
Science and Technology

Vasileios Gkioulos

Securing Tactical Service Oriented Architectures

Thesis for the degree of Philosophiae Doctor

Gjøvik, February 2018

Norwegian University of Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Information Security and Communication
Technology

NTNU
Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Information Technology
and Electrical Engineering
Department of Information Security and Communication
Technology

ISBN 978-82-326-2884-1 (printed version)
ISBN 978-82-326-2885-8 (electronic version)
ISSN 1503-8181

Doctoral theses at NTNU, 2018:46

Printed by Skipnes Kommunikasjon as

Securing Tactical Service Oriented Architectures

Vasileios Gkioulos

Thesis submitted to the
Norwegian University of Science and Technology

for the degree of Doctor of Philosophy in
Information Security

NTNU
Norwegian University of
Science and Technology

2018

Securing Tactical Service Oriented Architectures

Faculty of Information Technology and Electrical Engineering
Norwegian University of Science and Technology

"No man ever wetted clay and then left it, as if there would be bricks by chance and fortune."

(Plutarch, 45-120 A.D., Morals - De Fortuna)

Declaration of Authorship

I, Vasileios Gkioulos, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

(Vasileios Gkioulos)

Date:

Abstract

Research and development across military network technologies is an ongoing task, seeking to satisfy continuously evolving requirements and adversarial models. Beyond distinct implementations or technologies, the aforementioned requirements specify networks that provide, flexibility, agility, and adaptability to the dynamic military operational context. Furthermore, such networks must primarily support uninterrupted access to services and information, for the consolidation and maintenance of an enriched COP (Common Operational Picture), and the provisioning of military capabilities.

Nonetheless, military networks do not constitute a unified environment, for which generic technologies can be developed and deployed, while a clear distinction exists between the strategic, operational and tactical levels. The strategic/ operational levels rely on permanent or semi-permanent infrastructure that supports components such as headquarters, mission control centres, and logistics coordination centres. Contrary to that, the tactical level incorporates provisional assets deployed for the attainment of specific operational objectives, within singular or interlaced mission scenarios.

Therefore, tactical networks are of constrained nature in terms related to infrastructure, operational capabilities, and resource availability. Accordingly, deploying and securing tactical C2 (Command and Control) and C4I (Command, Control, Communications, Computers, and Intelligence) systems, must accommodate such requirements and constraints. Furthermore, the increased integration of information systems towards the attainment of NEC (Network Enabled Capability), promoted the use of SOA (Service Oriented Architectures) across all levels. To address the security challenges, imposed by tactical SOA, the scope of this thesis is tripartite.

Initially, the corresponding requirements have been extracted, referring both to the protection of information and services, but also to functional requirements for the developed policy and service architectures. Protecting tactical SOA requires the accommodation of security requirements, for stored, transmitted and processed information, under the explicit constraints of the tactical environment, maintaining operability within the various tactical modes of operation. Furthermore, the constraints of tactical networks impose significant limitations to the realization of suitable SOA based solutions. Overcoming these limitations, while maintaining the enforcement of security controls for the protection of services, as the means to process

information, is a critical task that we investigated. Finally the functional requirements for the implementation of a security policy mechanism tailored to tactical SOA, have been extracted and analysed.

The aforementioned constraints within the highly dynamic tactical environment, impose significant limitations to the functionalities and efficiency of current security policy frameworks. Thus, a security policy framework dedicated to tactical SOA is presented, as it has been developed in alignment to the previously identified requirements. Consequently, due to the constrained nature of tactical nodes, the parameters governing the partitioning and distribution of security policies are investigated within our work. Elements of critical impact have been identified and analysed, while a suitable partitioning mechanism has been defined. Furthermore, possible divergences across the distributed policies have been classified, and mechanisms for policy reconciliation have been developed. The nature of occurring divergences has been limited to an expected and permitted subset, while taking under consideration the constraints of the tactical environment and the requirement for auditing, prioritization and roll back capabilities.

The last component of our research relates to the development of a core security service architecture, tailored to the requirements of tactical SOA. This refers to a subset of services that are dedicated to the attainment of the identified security controls, according to security policies established at the mission preparation stage. Furthermore, additional aspects such as the interoperability of the security architecture and the QoS (Quality of Service) decision subsystem have been examined.

Sammendrag

Forskning og utvikling innen militære nettverksteknologier møter stadig økende krav og endrede sikkerhetsmodeller. Foruten spesifikke teknologiimplementasjoner er de nevnte kravene først og fremst knyttet til fleksibilitet, dynamikk og tilpasning til dynamiske militære operasjoner. Slike nettverk må hovedsakelig støtte uavbrutt tjeneste- og informasjonstilgang, sammenslåing og vedlikehold av et felles overordna stridsbilde (COP Common Operational Picture) og utrulling av militære ytelsesevner.

Militære nettverk utgjør ikke noe enhetlig miljø hvor generelle teknologier kan bli utviklet og utplassert og det eksisterer en klar forskjell mellom strategiske og taktiske domener. Det strategiske domenet innbefatter en permanent eller en halv-permanent infrastruktur som støtter opp under nettverkskomponenter for hovedkontor, operasjonskontrollsentere og logiske koordineringssentre. I motsetning, så innbefatter taktiske domener en mer provisorisk utrulling av enheter for oppnåelse av spesifikke operasjonelle mål innen enkle eller sammensatte militære operasjoner.

Taktiske nettverk er derfor naturlig begrenset i forhold til infrastruktur, operasjonelle evner og ressurstilgjengelighet. Utrulling og sikring av taktiske kommando og kontroll systemer (C2 Command and Control og C4I Command, Control, Communication, Computer and Intelligence) må derfor imøtekomme en rekke krav og har mange begrensninger. På grunn av en økende integrasjonsgrad mellom ulike informasjonssystemer for å oppnå NEC (Network Enabled Capability), promoteres tjenesteorientert arkitektur (SOA Service Oriented Architectures) for begge typer domener. For å på best mulig måte kunne adressere sikkerhetsutfordringene igjennom bruk av taktisk SOA, er omfanget i denne avhandlingen tredelt.

Den første delen inneholder relevante krav funnet for å kunne utføre beskyttelse på tjeneste og informasjon nivå, men det er i tillegg også satt funksjonelle krav relatert til vår utviklede policy og tjeneste arkitektur. Det å beskytte taktisk SOA setter sikkerhetskrav for lagret, sendt og prosessert informasjon, men det setter også eksplisitte begrensninger i taktiske miljø for å opprettholde stabil drift i ulike taktiske driftsmodus. Disse begrensningene av taktiske nettverk tvinger frem et begrenset utfallsrom av mulige SOA løsninger. Det å komme over disse begrensingene, samtidig som at sikkerheten håndheves for tjenestebeskyttelse innen informasjonsprosessering, er en kritisk oppgave som det har blitt forsket på. Kravdelen ble avsluttet ved

å ekstrahere og analysere en rekke funksjonelle implementasjonskrav til en sikkerhetspolicy spesialtilpasset til taktisk SOA.

Disse begrensingene innen dynamiske taktiske miljø, utgjør en signifikant innskrenking av eksisterende sikkerhetsrammeverk. Den andre delen av forskningen presenterer derfor et rammeverk for en sikkerhetspolicy satt opp for taktisk SOA, som har blitt utviklet i tråd med de identifiserte kravene. På grunn av en naturlig begrensning i taktiske noder, er det blitt forsket på parameterne som styrer partisjonering og distribusjon av sikkerhetspolicyer. Det har blitt analysert og identifisert elementer av kritisk betydning og det har blitt definert en passende partisjonersmekanisme. Mulige avvik for distribuerte policyer har blitt klassifisert og det har blitt utviklet en metode for å slå sammen og forsone sikkerhetspolicyer. Med tanke på begrensingene i det taktiske miljøet og kravene som er satt for revisjon, prioritering og tilbakerullingsmuligheter, så har naturlige avvikshendelser blitt begrenset til et forventet og tillatt utfallsrom.

Den siste delen i forskningen vår er relatert til utviklingen av en spesialtilpasset kjerne i en sikkerhetstjenestearkitektur som er laget på grunnlag av kravene ifra taktisk SOA. Det er gjort et relevant utvalg av tjenester som er satt til å oppnå en ønsket grad sikkerhetskontroll, i henhold til sikkerhetspolicyen som blir fastsatt i forberedelsesfasen av en militær operasjon. I tillegg er det også forsket på ulike aspekter rundt samspillingsevnen mellom sikkerhetsarkitekturen og deler av tjenestekvalitetssystemene (QoS Quality of Service).

Acknowledgments

"True friends are a sure refuge. The young they keep out of mischief; to the old they are a comfort and aid in their weakness, and those in the prime of life they incite to noble deeds."

(Aristotle, 384-322 B.C., Nicomachean Ethics)

Nothing comes from nothing, and it is a pleasure to thank all those who helped bringing this thesis to life, with their support, patience, and advice.

First and foremost I would like to thank my parents, for always being the greatest support to my endeavours, with understanding, encouragement and a helpful advice in any misfortune. Similarly, I would like to thank my teachers and professors during the early years of my studies, whose hard work and patience formed the basis of my professional character, and gave me the capacity to pursue my goals.

The completion of this PhD thesis being the latest of these goals, I would like to express my sincere gratitude to my principal supervisor Prof. Stephen D. Wolthusen. His insightful guidance and commitment into leading by example, allowed me to identify the true meaning of research and the fundamental purpose of academia. Through this, and by allowing me to explore additional research areas of my interest, I was given the opportunity to establish my personal stance within the academic community, and for this I will always be greatly indebted.

Furthermore, I would like to thank all the members of the Norwegian Information Security Laboratory, Center for Cyber and Information Security, and the COINS Research School of Computer and Information Security, for creating an excellent working environment. Including both the academic and administrative stuff, the fruitful discussions, cooperative spirit, and engaging character, facilitate healthy competition within a teamwork oriented group, being a member of which is a pleasure and honour.

Moreover, I would like to express my gratitude to my friends, whose company and encouragement has been a great support, and transformed Norway into a new and welcoming home. Last but not least I would like to thank my colleagues within the EDA (European Defence Agency) project TACTICS for an excellent cooperation, where scientific and management challenges have always been received and addressed with utmost professionalism.

Contents

List of Figures

List of Tables

List of Abbreviations

ACM:	Agile Computing Middle-ware
ALC:	Attribute Language with Complements
AoO:	Area of Operations
C2:	Command and Control
C4I:	Command, Control, Communications, Computers, and Intelligence
C4ISR:	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
COMINT:	Communication Intelligence
CoNSIS	Coalition Networks for Secure Information Sharing
COP:	Common Operational Picture
DL:	Description Logic
DTN:	Disruption Tolerant Networks
EDA:	European Defence Agency
ELINT:	Electronic Signal Intelligence
EMCON:	Emission Control
ENISA:	European Union Agency for Network and Information Security
ESB:	Enterprise Service Bus
FFI:	Forsvarets Forskningsinstitutt - Norwegian Defence Research Establishment
IED:	Improvised Explosive Device
IETF:	Internet Engineering Task Force
IoT:	Internet of Things
IS:	Information System
IST:	Information Systems Technology Panel
MANET:	Mobile ad-hoc networks
MEDEVAC:	Medical Evacuation
MIDNet:	Military Disruption Tolerant Networks
MoD:	Ministry of Defence
NATO:	North Atlantic Treaty Organization
NCW:	Network Centric Warfare
NEC:	Network Enabled Capability
NIST:	National Institute of Standards and Technology
ODMT:	Ontology Divergence Mapping Tree

OODA:	Observe, Orient, Decide, Act
OSI:	Open Systems Interconnect
OWL:	Web Ontology Language
PCIM:	Policy Core Information Model
PDP:	Policy Decision Point
PEP:	Policy Enforcement Point
QoI:	Quality of Information
QoS:	Quality of Service
RBAC:	Role Based Access Control
RSTA:	Reconnaissance Surveillance and Target Acquisition
RTO:	Research and Technology Organization
SatCom:	Satellite Communications
SOA:	Service Oriented Architectures
SOAP:	Simple Object Access Protocol
SQM:	Service Quality Management
SWRL:	Semantic Web Rule Language
TACTICS:	TACTICal Service oriented architectures
TRA:	Tactical Service Infrastructure Reference Architecture
TSI:	Tactical Service Infrastructure
TSPF:	Tactical Security Policy Framework
TSSI:	Tactical Security Service Infrastructure
UAV:	Unmanned Aerial Vehicles
UDDI:	Universal Description Discovery and Integration
UHF:	Ultra High Frequency
VHF:	Very High Frequency
XML Dsig:	XML Digital Signature
XML Enc:	XML Encryption
WIN:	War-fighter Information Network
WLAN:	Wireless Local Area Network
WS-Security:	Web Services - Security
WSDL:	Web Services Description Language

Chapter 1

Introduction

1.1 Motivation

The deployment of constrained networks is necessitated across multiple application domains, due to financial, technical, physical, and regulatory limitations. Examples of such application domains can be traced within tactical and emergency response networks, IoT (Internet of Things) systems, but also semi-autonomous networks deployed for remote ecosystem monitoring. Such systems are distributed and dynamic in nature, while characterized by resource limitations and intermittent connectivity towards backbone overprovisioned infrastructure.

Proportionally, tactical networks refer to collections of constrained terminals, deployed for the attainment of mission specific operational objectives. Nominally this primarily relies on ad hoc and mesh network configurations, with limited communication and processing capabilities in comparison to the (semi-) permanent infrastructure serving the strategic and operational levels. Therefore, deployment and integration of such networks with C2 and C4I systems at the tactical edge, must be suitably adjusted to these limitations, in order to accommodate information exchange and the provisioning of tactical capabilities.

Furthermore, the requirement for enabling NCW (Network Centric Warfare) and NEC across military networks has become imperative, necessitating the integration of decision-makers, information sources, and effectors. This has increased the heterogeneity and complexity of contemporary C2 and C4I systems, promoting the adoption of SOA as the most suitable mediator towards a modular and efficient information infrastructure. The SOA paradigm has been identified as a suitable solution, due to the inherent development and deployment flexibility of such architectures, where interoperability of services is utilised in order to achieve improved reactivity and situational awareness.

Nonetheless, contemporary SOA are focused primarily at the enterprise domain, where architectural models are defined mainly upon overprovisioned infrastructures and limited communication constraints. Therefore, although existing architectures may become adjusted for the infrastructures serving the strategic and operational levels, provided suitable adaptations to the military context, the tactical domain imposes a unique set of require-

ments that render such solutions inefficient. Accordingly, extending this paradigm to the tactical edge requires tailored solutions, which can accommodate the extended set of constraints and requirements, allowing tactical nodes to consume information and services locally, but also from and towards the infrastructure serving the strategic and operational levels.

1.2 Aim and Scope

Securing communication networks is a multifaceted objective, dependent upon several diverse yet interlaced tasks. These tasks range from the initial execution of risk analysis, to the deployment of suitable controls, and the establishment of incidence response mechanisms. Furthermore, application domains such as those described earlier, are attributed with two adjectives which are characteristic of their nature, namely *constrained* and *dynamic*. Accordingly, the efficiency and effectiveness of the deployed security solutions is decidedly bound to these two concepts. Within this study the focus is set on tactical SOA as a characteristic application domain of this nature. Accordingly, a selected fragment of topics, related to network security management have been investigated, towards securing the envisioned NEC and NCW enabled tactical networks.

Due to the aforementioned distinction between the infrastructure serving the tactical and strategic/ operational levels, universal solutions cannot be designed and optimized efficiently. This has been illustrated by early attempts to adapt enterprise SOA within military networks. Such solutions have been proven capable of satisfying the requirements of the overprovisioned infrastructure deployed across the strategic and operational levels, while experience from recent battlefields suggest that the tactical edge requires a distinct approach. Accordingly, the deployed SOA must be suitably adjusted to the available resources, operational characteristics, and required functionalities of each domain. Seeking to obtain refined security control across tactical SOA demands a comprehensive analysis of their characteristics, requirements and underlying constrains. This can ensure that the developed components can efficiently satisfy the functional preconditions raised by the nature of modern AoO (Areas of Operations), and national planning for future strategic objectives.

These components refer to the security services that constitute the developed TSSI (Tactical Security Service Infrastructure), which must accommodate both the extraction of pertinent policy decisions, and their enforcement by the deployed control subsystems. A critical factor in respect of the TSSI, refers to the adaptability to dynamic network conditions, which must be maintained across the various deployed platforms and operational conditions. This requirement is necessitated by the disparate nature of the platforms deployed at the tactical domain, and the unpredictability factor that

is bound to any military operation.

Finally, policy mechanisms constitute a core component of every security architecture, dedicated to the governance of the deployed control subsystems for the attainment of the required protection goals. Accordingly, the developed TSPF (Tactical Security Policy Framework) must rely on solutions with demonstrated efficacy, suitably adjusted to the tactical context, according to the previously identified constraints and requirements. The supported security policies should efficiently utilize the available network resources and cross-layer information, in order to facilitate the adaptability of the TSI (Tactical Service Infrastructure) to the dynamic network condition.

1.3 Research Questions

This study was driven by the research questions listed bellow, which have been formulated in alignment with the aforementioned motivation and scope. The results described in this work were obtained from the security related fragment of the EDA (European Defence Agency) project TACTICS (TACTICal Service oriented architectures). The overarching goal of TACTICS has been to provide a proof of concept, in respect of the capacity of contemporary tactical networks to support the deployment of SOA, under the realistic constraints of current and potential future AoO.

- *1st Research Question:* Which are the operational and technical requirements for the attainment of fine-grained security goals within tactical SOA, under the constraints imposed by the characteristics of contemporary and future tactical operations?

- *2nd Research Question:* Which are the required architectural components and functionalities, for the enforcement of security controls within contemporary tactical SOA?

- *3rd Research Question:* How can a policy that is sufficiently expressive to allow the incorporation of discretionary access control, be formulated and implemented in a way that can satisfy the security requirements and constraints of tactical SOA?

- *4th Research Question:* Given the results of the previous research questions, and a suitable reference architecture, can contemporary tactical networks support the deployment of security architectures developed according to the SOA paradigm?

1.4 Background

1.4.1 Network Centric Warfare/ Network Enabled Capability

NCW (source: United States Department of Defence) and NEC (source: United Kingdom Ministry of Defence) are two military doctrines that share core tenets, and seek to integrate information sources, decision makers and effectors. This is expected to enhance reactivity on the battlefield, by optimizing asset utilization towards overwhelming and synchronized effect. Alberts et al. [32] provide a detailed report over the concept of NCW, and how it is envisioned to contribute towards developing and leveraging information superiority on the battlefield. As stated by the authors: *"We define NCW as an information superiority enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battle-space."*

1.4.2 Constrained networks

RFC7228 and RFC7547 [13, 30] provide a comprehensive description of the terminology and concepts related to constrained networks. Although the tactical environment presents a wider scope in respect of the utilised terminals and network operational characteristics, these two documents closely formalize the lowermost boundary of operation. Accordingly within this thesis, the following definitions are used as extracted from the aforementioned documents:

Constrained Node: *A node where some of the characteristics that are otherwise pretty much taken for granted for Internet nodes at the time of writing are not attainable, often due to cost constraints and/ or physical constraints on characteristics such as size, weight, and available power and energy. The tight limits on power, memory, and processing resources lead to hard upper bounds on state, code space, and processing cycles, making optimization of energy and network bandwidth usage a dominating consideration in all design requirements. Also, some layer-2 services such as full connectivity and broadcast/ multicast may be lacking.*

Constrained Network: *A network where some of the characteristics pretty much taken for granted with link layers in common use in the Internet at the time of writing are not attainable. Limitations can include:*

1. *Low achievable bitrate/ throughput.*
2. *High packet loss and packet loss variability.*
3. *Highly asymmetric link characteristics.*

4. *Severe penalties for using large packets.*
5. *Limits on reachability over time.*
6. *Lack or severe constraints on advanced services, such as IP multicast.*

Challenged Network: *A network that has serious trouble maintaining what an application would today expect of the end-to-end IP model by:*

1. *Not being able to offer end-to-end IP connectivity at all.*
2. *Exhibiting serious interruptions in end-to-end IP connectivity.*
3. *Exhibiting delay well beyond the Maximum Segment Lifetime.*

All challenged networks are constrained networks in some sense, but not all constrained networks are challenged networks, while there is no well-defined boundary between the two.

Constrained-Node Network: *A network whose characteristics are influenced by being composed of a significant portion of constrained nodes. A constrained-node network always is a constrained network because of the network constraints stemming from the node constraints, but it may also have other constraints that already make it a constrained network.*

The tactical level relies on infrastructureless constrained networks of mobile devices, with self configuring characteristics, and intermittent connectivity towards the strategic and operational levels, which contrary to that, rely on a combination of comparatively overprovisioned wireline and wireless networks. It must be noted that not all types of tactical nodes are constrained, while sections of the network can operate under a non-constrained/non-challenged mode. Nevertheless, the overall network architectures are of constrained nature primarily owing to the:

1. Rate of change and unpredictability component within the network topology graph.
2. Lack of predominant traffic flow models, which are primarily bound to mission specific parameters.
3. Bandwidth and bit error rate limitations, largely due to bottlenecks created by constrained devices.
4. Reliance on distributed or hierarchical network management.

*NOTE: For the remainder of this thesis the term "tactical domain" will refer to the heterogeneous and constrained infrastructure deployed for the facilitation of the objectives that fall under the responsibility of the tactical operational level. Further, the term "strategic domain" will refer to the overprovisioned (comparatively to the tactical) infrastructure deployed for the facilitation of the objectives that fall under the responsibility of the operational and strategic levels.

1.4.3 Service Oriented Architectures

Townsend [75] reports the history and intensives that led to the development of the SOA paradigm, as a method of decomposing system functionalities into a structured subset of interoperable services, since the early 80s. Currently, SOA terminology and core concepts are formalized within ISO/IEC 18384 in three documents:

1. Part 1: Terminology and Concepts for SOA [1].
2. Part 2: Reference Architecture for SOA solutions [2].
3. Part 3: Service Oriented Architecture Ontology [3].

Extracting from these documents, the following concepts are used within this thesis:

Architecture: *Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution.*

Choreography: *Type of composition whose elements interact in a non-directed fashion with each autonomous part knowing and following an observable predefined pattern of behaviour for the entire (global) composition. Choreography does not require complete or perfect knowledge of the pattern of behaviour.*

Collaboration: *Type of composition whose elements interact in a non-directed fashion, each according to their own plans and purposes without a predefined pattern of behaviour.*

Composition: *Result of assembling a collection of elements for a particular purpose.*

Element: *Unit at a given level of abstraction and with a clearly defined boundary. An element can be any type of entity.*

Entity: *Individual element in a system with an identity which can act as a service provider or service consumer. Examples of entities are organizations, enterprises and individuals, software, and hardware.*

Orchestration: *Type of composition where one particular element is used by the composition to oversee and direct the other elements. The element that directs an orchestration is not part of the orchestration (composition instance) itself.*

Policy: *Statement that an entity intends to follow or intends that another entity should follow.*

Process: *Type of composition whose elements are composed into a sequence or flow of activities and interactions with the objective of carrying out certain work. A process may also be a collaboration, choreography, or orchestration.*

Service: *Logical representation of a set of activities that has specified outcomes, is self-contained, may be composed of other services, and is a black box to consumers of the service.*

Service composition: *Service assembly composition that provides (in the operational sense) higher level services that are only an assembly of other services.*

Service consumer: *Entity that uses services. Consumers may interact with services operationally or contractually (legal responsibility).*

Service interoperability: *Ability of service providers and service consumers to communicate, invoke services and exchange information at both the syntactic and semantic level leading to effects as defined by the service description.*

Service Level Agreement/ SLA: *Type of service contract that defines measurable conditions of interactions between a service provider and a service consumer.*

Service orientation: *Approach to designing systems in terms of services and service-based development.*

Service Oriented Architecture/ SOA: *Architectural style that supports service orientation and is a paradigm for building business solutions. Services realized in this style utilize activities that comprise business processes, have descriptions to provide context, may be implemented via service composition, have environment-specific implementations which are described in the context that constrains or enables them, require governance, and place requirements on the infrastructure to achieve interoperability and location transparency using standards to the greatest extent possible.*

Service provider: *Entity providing services. Service providers may be responsible for the operation of the services or the contract for the services (legal responsibility) or both.*

SOA implementation: *Methods and techniques used to develop SOA based solutions.*

1.4.4 Policy based security management

A recommended terminology for policy-based management is defined in RFC 3198 [84]. Extracting from this document, the following terms are applicable for this thesis.

Policy: *"Policy" can be defined from two perspectives:*
- A definite goal, course or method of action to guide and determine present and future decisions. "Policies" are implemented or executed within a particular context (such as policies defined within a business unit).
- Policies as a set of rules to administer, manage, and control access to network resources.
These two views are not contradictory since individual rules may be defined in support of business goals.

Policy abstraction: *Policy can be represented at different levels, ranging from business goals to device-specific configuration parameters. Translation between different levels of "abstraction" may require information other than policy, such as network and host parameter configuration and capabilities.*

Policy action: *Definition of what is to be done to enforce a policy rule, when the conditions of the rule are met. Policy actions may result in the execution of one or more operations to affect and/or configure network traffic and network resources.*
*Note: The enforcement direction of this definition can be bilateral, bound to

whether the independent variable is the "rule conditions" or the "enforced action". For the purpose of this thesis, and within the developed security mechanisms, both enforcement directions are available.

Policy condition: *A representation of the necessary state and/ or prerequisites that define whether a policy rules actions should be performed. This representation need not be completely specified, but may be implicitly provided in an implementation or protocol. When the policy condition(s) associated with a policy rule evaluate to TRUE, then (subject to other considerations such as rule priorities and decision strategies) the rule should be enforced.*

Policy conflict: *Occurs when the actions of two rules (that are both satisfied simultaneously) contradict each other. The entity implementing the policy would not be able to determine which action to perform. The implementers of policy systems must provide conflict detection and avoidance or resolution mechanisms to prevent this situation.*

Policy decision: *Two perspectives of "policy decision" exist:*
- A "process" perspective that deals with the evaluation of a policy rules conditions.
- A "result" perspective that deals with the actions for enforcement, when the conditions of a policy rule are TRUE.

Policy domain: *A collection of elements and services, and/ or a portion of an Internet over which a common and consistent set of policies are administered in a coordinated fashion. This definition of a policy domain does not preclude multiple sources of policy creation within an organization, but does require that the resultant policies be coordinated. Policies defined in the context of one domain may need to be communicated or negotiated outside of that domain.*

Policy enforcement: *The execution of a policy decision.*

Policy error: *"Policy errors" occur when attempts to enforce policy actions fail, whether due to temporary state or permanent mismatch between the policy actions and the device enforcement capabilities.*

Policy goal: *Goals are the business objectives or desired state intended to be maintained by a policy system. As the highest level of abstraction of policy, these goals are most directly described in business rather than technical terms.*

Policy request: *A message requesting a policy-related service. This may refer to a request to retrieve a specific set of policy rules, to determine the actions to enforce, or other policy requests.*

Policy rule: *A basic building block of a policy-based system. It is the binding of a set of actions to a set of conditions, where the conditions are evaluated to determine whether the actions are performed.*

Furthermore, RFC 3060 [55] specifies PCIM (Policy Core Information Model), which is an object oriented model for the representation of policies. This document defines core concepts of policy driven management, and an architecture which has been adapted and utilised across multiple commercial products. A classification of policies is provided, which has been utilised across this thesis. Extracting from the document, policies can

be classified according to their purpose as:

Motivational Policies: *Solely targeted at whether or how a policy's goal is accomplished. Configuration and Usage Policies are specific kinds of Motivational Policies. Another example is the scheduling of file backup based on disk write activity from 8am to 3pm.*

Configuration Policies: *They define the default (or generic) setup of a managed entity (for example, a network service). Examples of Configuration Policies are the setup of a network forwarding service or a network-hosted print queue.*

Installation Policies: *They define what can and cannot be put on a system or component, as well as the configuration of the mechanisms that perform the install. Installation policies typically represent specific administrative permissions, and can also represent dependencies between different components (e.g., to complete the installation of component A, components B and C must be previously successfully installed or uninstalled).*

Error and Event Policies: *For example, if a device fails between 8am and 9pm, call the system administrator, otherwise call the Help Desk.*

Usage Policies: *They control the selection and configuration of entities based on specific "usage" data. Configuration Policies can be modified or simply reapplied by Usage Policies. Examples of Usage Policies include upgrading network forwarding services after a user is verified to be a member of a "gold" service group, or reconfiguring a printer to be able to handle the next job in its queue.*

Security Policies: *They deal with verifying that the client is actually who the client purports to be, permitting or denying access to resources, selecting and applying appropriate authentication mechanisms, and performing accounting and auditing of resources.*

Service Policies: *They characterize network and other services (not use them). For example, all wide-area backbone interfaces shall use a specific type of queuing. Service policies describe services available in the network. Usage policies describe the particular binding of a client of the network to services available in the network.*

1.4.5 Cross-layer security

Srivastava and Motani [68] provide detailed definitions and description for layered and cross-layer architectures. Extracting from this document, these terms are utilised across this thesis, as:

Layered architecture: *A layered architecture, like the seven-layer OSI (Open Systems Interconnect) model, divides the overall networking task into layers and defines a hierarchy of services to be provided by the individual layers. The services at the layers are realized by designing protocols for the different layers. The architecture forbids direct communication between non-adjacent layers; communication between adjacent layers is limited to procedure calls and responses.*

Cross-Layer architecture: *Protocol design by the violation of a reference layered communication architecture is cross-layer design with respect to the particular layered architecture.*

Comment 1: Examples of violation of a layered architecture include creating new interfaces between layers, redefining the layer boundaries, designing protocol at a layer based on the details of how another layer is designed, joint tuning of parameters across layers, and so on.
Comment 2: Violation of a layered architecture involves giving up the luxury of designing protocols at different layers independently. Protocols so designed impose some conditions on the processing at other layer(s).
Comment 3: Cross-layer design is defined as a protocol design methodology. However, a protocol designed with this methodology is also termed cross-layer design.

Furthermore Conti et al. [23] and Saleem et al. [58], analyse the rationale that promoted the use of cross-layer architectures, particularly within mobile ad hoc networks, providing exemplary detailed applications. According to the authors: *"Why does the presence of wireless links in the network motivate designers to violate the layered architectures? There are three main reasons: the unique problems created by wireless links, the possibility of opportunistic communication on wireless links, and the new modalities of communication offered by the wireless medium."* Therefore, state information for a particular layer are used in order to optimise the behaviour of another, allowing for refined network governance and enhanced performance within the constrains of such network architectures.

Accordingly, multiple studies applied this paradigm within the realm of security across constrained wireless networks [82, 62, 6], while concerning military applications a related study from FFI (Forsvarets Forskningsinstitutt) [43] concludes with: *Cyber Defence is classic and static information security often based on cryptographic techniques, while Cyber Security aids the dynamical handling of concrete incidents and attacks. Many aspects of Cyber Security can be handled in a single layer, but activities are in principle cross-layer. Whether an operation is defensive or offensive, the ability to analyse or control all aspects of the data is a valuable asset. A typical example is an intrusion detection system where traffic is analysed from many different layers and perspectives. In Cyber Defence, security mechanisms are usually applied at one layer at a time. This means that a mechanism like encryption is often applied independently at different layers. This gives added security in depth, since an attacker will have to circumvent several mechanisms to attack the system.*

1.4.6 Ontological knowledge representation

Guarino et al. [37] discuss in depth the concept of ontologies, for which the original definition was given by Gruber [36], as: *"A specification of a representational vocabulary for a shared domain of discourse definitions of classes, relations, functions, and other objects is called an ontology. An ontology is an explicit specification of a conceptualization."*

Accordingly, conceptualization was defined by Genesereth and Nilsson [33], as: *"A body of formally represented knowledge is based on a conceptualiza-*

tion: the objects, concepts, and other entities that are assumed to exist in some area of interest and the relationships that hold among them. A conceptualization is an abstract, simplified view of the world that we wish to represent for some purpose. Every knowledge base, knowledge-based system, or knowledge-level agent is committed to some conceptualization, explicitly or implicitly."

Ontologies are formalised with the use of ontology specification languages, which are primarily based on traditional syntax, markup schemes, frame schemes, description logic, or first order logic. The principal distinction among these languages arise from their expressive capacity and supporting reasoning capabilities, where a semantic reasoner can be used in order to infer logical consequences from the axioms defined within an ontology.

Regarding the expressive capacity of ontology specification languages, OWL (Web Ontology Language) can be used as an example. Extracting from [10]: *The OWL language provides two specific subsets that we believe will be of use to implementors and language users. [] OWL Full and OWL DL support the same set of OWL language constructs. Their difference lies in restrictions on the use of some of those features and on the use of RDF features. OWL Full allows free mixing of OWL with RDF Schema and, like RDF Schema, does not enforce a strict separation of classes, properties, individuals and data values. OWL DL puts constraints on the mixing with RDF and requires disjointness of classes, properties, individuals and data values. The main reason for having the OWL DL sublanguage is that tool builders have developed powerful reasoning systems which support ontologies constrained by the restrictions required for OWL DL. [] OWL Lite is a sublanguage of OWL DL that supports only a subset of the OWL language constructs. OWL Lite is particularly targeted at tool builders, who want to support OWL, but want to start with a relatively simple basic set of language features. OWL Lite abides by the same semantic restrictions as OWL DL, allowing reasoning engines to guarantee certain desirable properties.*

1.5 Related Work

1.5.1 Tactical Networks Towards NEC and NCW

Military networks have been continuously studied since their first appearance, seeking to improve situational awareness, decision making, and the efficient/effective utilization of the capabilities supported by the deployed assets. This includes a wide range of research domains, from generic studies over the characteristics of military operations, up to system or technology specific studies aiming to satisfy explicit requirements.

Indicatively, Aschenbruck et al. [5] examine scenarios of military operations and natural or man-made catastrophes, where the lack or destruction of backbone infrastructure impedes communications. Maintaining readi-

ness for such events requires the execution of field trials and simulations, whose correctness relies on the accuracy of the utilized mobility models. The authors provide a generic classification of existing mobility models for tactical networks, including an analysis of their characteristics and dependencies. The authors conclude, according to the examined tactical scenarios, that the disaster-area-model is the one which realises more accurately the features of tactical networks, approximating closely the realistic boundaries of such systems. Nevertheless, the authors highlight the need for developing more precise and scalable models in the future. Furthermore, Li and Vigneron [49] utilize realistic network deployment scenarios and mobility models in order to investigate the link and network properties over VHF combat radios. A model is proposed according to practical deployment scenarios, highlighting the inherent dynamicity of tactical networks that necessitate the adaptability of deployed architectures to the underlying constraints. Elmasry [29] compares commercial and tactical wireless networks, seeking to identify differences in their requirements and constraints. The article highlights the additional obstacles imposed by the tactical environment, in terms of complexity, lack of fixed infrastructure, mobility patterns, and dynamicity. Furthermore, the author proposes a generic tactical network model according to the identified characteristics, seeking to promote technological spillovers from commercial networks, in areas where this is deemed feasible.

Moreover, Cheng et al. [20] focus on airborne tactical networks, providing a comprehensive analysis of design considerations for such systems at the physical, link and network layers. These include the support of variable data rates, provisioning of multicast traffic, latency constraints, and long transmission ranges. Research on the field also focused on the adaptation of equipment to the tactical environment, such as Kaul et al. [45] who investigated the capacity of commercial smart-phones to participate into tactical networks, aiming to satisfy the identified constraints. Under the main considerations of supporting IP multicast, and tactical mobility patterns, the authors investigate and introduce novel technologies towards adapting commercial mobile equipment to the tactical edge.

Furthermore, analysis of the tactical environment has also been focused on the adaptation of specific technologies. Suri et al. [71] report results from experiments on tactical networking environments, with service deployment over peer-to-peer communications. The article presents and discuss requirements for a peer-to-peer middleware at the tactical edge, such as automatic configuration, bandwidth efficiency, and peer discovery. This study includes experimental results that support the identified requirements, and the capacity of peer-to-peer systems to operate under the constraints of the tactical environment. Furthermore, Sterbenz et al. [69] discuss the topic of survivability for mobile wireless networks, with particular empha-

sis on military applications. Although the scope of the article is related to QoS (Quality of Service) and routing aspects, the analysis provided by the authors forms a cohesive representation of the communication constraints imposed by the nature of tactical networks. In terms of security the authors highlight areas such as transmission security, communication security, access control, infrastructure protection, robustness, and efficiency, as the areas where future work should focus, seeking to provide effective solutions. Finally, Sioutis [65] investigated key technologies, challenges, and potential solutions for achieving seamless interoperability between the tactical and strategic domains within SOA. The author presents and investigates various tactical scenarios, providing a high level but comprehensive analysis of the challenges involved towards such integration. As stated by the author: *Tactical to enterprise integration is a complex problem which expands beyond simple network connectivity, or even information interoperability.* The challenges identified within this study, highlight the requirement for an effective information management and decision making subsystem, which would be able to support the tactical capabilities and requirements of the modern battlefield, through NCW/ NEC enabled tactical SOA.

Moving towards the NCW and NEC paradigms, multiple studies investigated the capacity of tactical networks to support the required functionalities and enhanced integration of information systems. Scott [60] investigated how DTN proxies at the application layer can support NCW over disrupted networks, while Burbank et al. [17] provided a comprehensive analysis of the tactical environment in terms of deployed units and their capabilities. Accordingly, the authors argue that MANETs (Mobile ad hoc networks) will have to face multiple challenges in order to support all the envisioned functionalities for providing NCW at the tactical edge. At the time this study was undertaken, the authors concluded that MANET technologies were still immature and not able to efficiently support this goal.

Furthermore, Bar-Noy et al. [7] motivated the need for a formal QoI (Quality of Information) metric for decision makers at the tactical edge, and the need for tactical networks not only to facilitate information flow, but also to incorporate suitable processes for distributed decision making according to such metrics. The authors discuss critical aspects in respect of assuring information provenance and credibility, as the the main challenges towards the envisioned QoI aware military networking. Mazzini et al. [54] investigated the opportunistic dissemination of information over tactical networks, under the identified constraints, suggesting algorithmic solutions for the extraction of network state information from the interaction of tactical nodes. The results of this study are promising in respect of improving reliability over data delivery with reduced bandwidth consumption. Finally, Suri et al. [70] investigated the limitations of tactical networks in terms of reliable connectivity, bandwidth availability and latency, exploring the notion

of Value-of-Information for improving communications. Accordingly, information are prioritized or filtered prior to be disseminated to field forces. The study shows promising initial results in respect of bandwidth reduction, highlighting the significance of fine-grained information management at the tactical edge.

Focusing on the security aspects of tactical ad hoc and mesh networks, a multitude of studies investigated generic [18, 78, 15, 14, 51, 57, 48] and system specific parameters [83, 34, 16, 50, 81, 35, 12]. Zhou and Haas [87] investigated the security requirements of ad hoc networks across military applications. Although the focus of this study is generically on the applications of ad hoc networks, it provides a comprehensive threat model, and analysis in respect of secure routing and key management. The authors highlight the network dynamicity, scalability and dependency on unreliable wireless links, as the main challenges towards achieving the corresponding security goals. Moreover, Jacobs [41] examined tactical networks, identifying the types of potential adversaries, threats and vulnerabilities, against the WIN (Warfighter Information Network). Finally, an overview of cryptographic methods is provided by the author, towards mitigating the identified risks. Furthermore, Kong et al. [47] present and evaluate their design for a multilevel ad hoc wireless network, utilizing UAVs (Unmanned Aerial Vehicles) to maintain connectivity after damages have occurred to the main network infrastructure. The article focuses on aspects related to message privacy, message integrity, non-repudiation, authentication, and security service availability, and how these can be supported within military networks.

Chlamtac et al. [21] investigated mobile ad hoc networking and its application to the military domain. An in depth analysis of the characteristics of such networks is provided by the authors, in terms of existing applications and adopted technologies. The focus of the article is not primarily on security, but it provides a comprehensive analysis of the integrated technologies at the time of this study, and a historical overview of their development. Cayirci and Rong [19] are the authors of a book entitled "Security in wireless ad hoc and sensor networks". The book provides a comprehensive analysis of security aspects related to ad hoc and sensor networks, including military applications. Both fundamental networking and operational characteristics are investigated, while an extensive analysis of related security topics is provided. These include secure routing, threats and countermeasures, as well as aspects related to cryptography and key management. Additionally, Yi et al. [86] focused on wireless mesh networks, and provided a survey of potential threats and available countermeasures. The authors focus on the areas of key management, intrusion detection, and secure routing. Nevertheless, the article presents a comprehensive overview of the security challenges for this type of networks. Finally, Kidston et al. [46] identified differences be-

tween commercial and tactical networks, utilizing their findings in order to provide a high-level analysis of threats and risks in tactical environments. This study also suggests a cross-layer security framework, as the medium to improve security within tactical networks, given the constraints that the author identify earlier.

Investigating the security aspects of tactical SOA, Maule and Lewis [53] present a methodology for assessing tactical maritime SOA performance, and discuss security challenges of such systems. A test architecture is described and utilized within a case study for the identification of latency sources, when web services are secured by means of certificates, in distributed SOA environments. Sauer et al. [59] investigated multiple approaches for cross-domain secure information sharing under collaborative and joint coalition SOA environments. The authors conclude that a truly efficient and effective solution would require a singular multi-level security SOA, which can be replicated across both the strategic and tactical domains. Furthermore Simanta et al. [63] described and demonstrated a set of prototypes for the deployment of SOA on hand-held devices at the tactical edge. Despite being a prototypical early stage implementation, this study provides an overview of engineering issues related to the involved technologies. The identified issues include the collection and dissemination of information, reliability, and improvements in the service discovery mechanisms. Additionally, Barz and Quinkert [9] presented the results of their studies, within the project CoNSIS (Coalition Networks for Secure Information Sharing), aiming to facilitate the exchange of information within tactical coalition environments. This article proposes a model for managing the interactions between tactical routers and security gateways. Finally Wang et al. [80] proposed a trust management protocol for task assignment in autonomous mobile ad hoc networks operating within service oriented architectures. The proposed algorithm is based on task auctioning, and is optimized according to local knowledge. The results show improved performance and minimized complexity, providing suitable ground for further enhancement with improved selection strategies.

1.5.2 SOA at the Tactical Edge

Earlier national and international studies have initiated the investigation, towards the adoption of the SOA paradigm across the tactical domain. The focus areas of these studies are disperse, referring to QoS, service delivery or management of coalition operations, while security aspects have also been studied.

MIDNet [52] (Military Disruption Tolerant Networks) is an EDA project focused on military DTN (Disruption Tolerant Networks), seeking to investigate the applicability of technologies developed within the DTN research community across the tactical domain. The overarching goal of this project

was the definition of a suitable DTN architecture, tailored to the specific requirements of tactical networks. Although the scope of TACTICS is distinct from MIDNet, the results of the later confirmed that standard tactical applications (such as e-mail, and blue force tracking) can be adjusted and integrated into the highly constrained tactical environment. In respect of security, the applicability of existing solutions such as WS-Security have been examined, identifying constraints and limitation under the examined scenarios.

Furthermore, under the support of the United States Army and Air Force, Suri et al. [73, 72] developed ACM (Agile Computing Middle-ware), which aims to improve the performance of constrained tactical networks by opportunistic resource exploitation. Again the focus of this project has been on performance optimization by utilizing unengaged network resources, without a direct orientation towards security. Nevertheless, the undertaken studies provide a comprehensive understanding of functionalities with security implications, such as service delivery management and network reliability.

Within NATO (North Atlantic Treaty Organization), RTO/ IST-061 (Research and Technology Organization/ Information Systems Technology Panel) [4] investigated security aspects of SOA towards the attainment of NEC. A variety of existing standards used for the development of SOA have been evaluated through analysis and experimentation, including WSDL (Web Services Description Language), SOAP (Simple Object Access Protocol), UDDI (Universal Description Discovery and Integration), XML Dsig (XML Digital Signature), XML Enc (XML Encryption), and WS-Security (Web Services Security). Valuable findings have been attained from this work, in respect of securing tactical SOA with methods available at that time, while the following extract from the final report provides a coherent summary: *"During the demonstration it became clear that current standards and implementations are not yet mature enough for operational deployment on a large scale. Even though products may claim to support a given standard, interoperability with other implementations of that standard is not always possible. Also, quite a few standards in the area of SOA are not yet stable or lack important features such as security considerations." [4]*

CoNSIS [8] has been an international research project, in cooperation between France, Germany, Norway and the United States of America. The projects' focus was the investigation, development and demonstration of technologies that can facilitate secure information sharing across tactical coalition environments, in alignment with contemporary NEC enabling methods. Although the scope of CoNSIS was not the development of an integrated security architecture, the undertaken studies provide useful insights into the related security considerations, such as key management, traffic flow confidentiality, and communication protection between military and civilian networks. CoNSIS utilized components from the earlier German

SOA RuDi [61], which was an early national project aiming to provide interoperability between web services within military environments. In respect of security, the core component has been the protection of information, which occurs at the network layer, while SOAP message encapsulation is used to protect messages during transmission.

FFI also released results from their studies, in adopting the SOA paradigm across military networks, within the FFI project 1277 [11]. In respect of security, a subset of standards has been investigated related to access control and identity management. The study focuses on standards currently evaluated by NATO (e.g. XACML, SAML, WS-Policy, XML Encryption, and IPSec), providing valuable results in respect of the corresponding challenges, required optimizations, and recommendations for future work. The results of this study convey the requirement for adaptable and refined security management, with optimizations towards the reduction of the security overhead. These early studies over military and tactical SOA, formed the basis and necessitated TACTICS, as a project that will develop a unified and complete SOA dedicated to the tactical domain.

1.5.3 Security Policies for Tactical Networks

In 2007, NIST (National Institute of Standards and Technology) published a technical report [64] with recommendations on web service security. The report is not focused on military applications, and in extend not adjusted to the corresponding constraints and requirements of the tactical environment. Nevertheless, the report provides essential insights on SOA security at the enterprise domain, and has been utilized as the basis for early military oriented studies and applications. As stated in the report: *The security challenges presented by the Web services approach are formidable and unavoidable. Many of the features that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are at odds with traditional security models and controls. [] Web services are increasingly becoming an integral part of organizational information technology (IT) infrastructures even though there are still unmet security challenges. To this end, the development and deployment of secure Web services is essential to many organizations' IT infrastructures. However, Web service security standards do not provide all of the required properties to develop robust, secure, and reliable Web services. To adequately support the needs of the Web services based applications, effective risk management and appropriate deployment of alternate countermeasures are essential. Defence in depth through security engineering, secure software development, and risk management can provide much of the robustness and reliability required by these applications.*

Wies [85] provides a general classification of policy mechanisms and a firm theoretical analysis of related concepts, such as policy life-cycle and level of abstraction. The latter is crucial for the specification of layered

policy-based management mechanisms, given the required separation of duty between the distinct components of such a system. The author provides the following clarification: *"The level of abstraction in terms of the desired behaviour of distributed heterogeneous systems, applications, and networks, depends on the degree of detail contained in the policy definition and the ratio of business related aspects to technological aspects within the policy. [] Thus policies do not describe business goals but are derived from them."* Accordingly, the described hierarchy provides a distinction between the layers of a policy-based management mechanism, separating *corporate (high level)*, *task oriented (acting as management tools)*, *functional (acting as management services)*, and *low level (acting as managed objects)* policy sub-components.

Accordingly, a multitude of policy-based management approaches have been developed, both for network [25] and security governance [67, 38, 26], focusing on specific application domains or policy abstraction layers. Tonti et al. [74] evaluated policy-based management frameworks based on semantic web languages for policy representation and reasoning, to non semantic web-based approaches (using Ponder as the framework for their comparisons). The authors describe and compare KAoS [77], Rei [44], and Ponder [27] within a communication control case study, on the grounds that these policy specification approaches have been targeted to distributed multi-agent systems. The study concludes that: *"Each form of policy representation exhibits pros and cons, and thus the choice of an approach should be driven by the characteristics of the application domain and by the application requirements. However, our experience to date seems to indicate quite clearly that, apart from the specific considerations of the representation employed, the adoption of Semantic Web representations provide more advantages than drawbacks."* The advantages of such approaches identified by the authors include:

1. Improved global expressiveness.
2. Capacity to represent complex environments, in terms of entities, concepts, interactions, and behaviours.
3. Conceptualization across multiple abstraction layers.
4. Easy and efficient extensibility. (Also at runtime)
5. Simplified policy querying, reasoning, and deconflictation.

The authors also identify areas where further improvements are needed such as the ease of deployment, use, and enforcement.

Furthermore, Duflos et al. [28] provide a comparative study over policy specification languages for secure distributed applications, examining ASL [42], Automated manager [66], DLSS [24], ISPS [31], LaSCO [40], Ponder [27], SPSL [22], and TOWER [39]. The study is structured over a com-

parative analysis for the capacity of the aforementioned policy specification approaches to define:

1. Access control.
2. Identification and authentication.
3. Confidentiality and integrity.
4. Obligations and prohibitions.
5. Auditing.
6. Delegation of privileges.

Within this analysis, Ponder is identified as the most complete framework, although it lacks a more refined definition of integrity and confidentiality. Furthermore, this study compares the levels of abstraction, and availability of feedback/ mapping mechanisms. Under these evaluation criteria, HQML was identified as the most complete framework, being able to support:

1. User/ application level specification.
2. Middle-ware/ network level specification.
3. Mapping mechanisms.
4. Feedback mechanisms.

Finally, the study investigates the corresponding policy representation techniques of each framework, and the utilized notions (e.g. Domain, Role, Group). The authors conclude with: *"For distributed application such as e-commerce the best language does not exist yet. It should be a mix of:*

- *Ponder, ISPS and SPSL for the suitability for specification of security.*
- *HQML for its different abstraction level to represent policy, the ability to map between these different levels and to give feedback to the higher level of abstraction.*
- *Ponder, ISPS and PPL for the technique used to represent policies.*
- *ASL, ISPS, and Ponder for their deconflictation capabilities.*
- *PDN, Ponder and DLSS for their capability to trigger the policies using both proactive and reactive approaches."*

Focusing on service oriented systems, Phan et al. [56] evaluated the IETF (Internet Engineering Task Force) PCIM [55], Ponder [27], KaOS [77], Rei [44], and WS-Policy [79], based on criteria and requirements specific to SOA. The examined criteria across this study have been:

1. Policy specification, analysis and enforcement.
2. Language formal semantics and extensibility.
3. Domains and other forms of grouping.
4. Support of distributed policy enforcement.
5. Meta policy (*Policy about policies*).
6. Business oriented policy specification.
7. The capacity to support dynamic system alterations.
8. Policy derivation from service composition.

The authors conclude with: *"It can be seen that none of the frameworks are readily applicable for SOA policy management because they are all short of some important features."* For PCIM this is attributed to the lack of formal specification language and services, while Ponder lacks the capacity to support dynamic system alterations and on-line service composition. Finally, according to their analysis the authors conclude that: *"WS-Policy is a low-level policy language that is specific to Web Services implementation and is not suitable for managing an overall SOA system."* The article identifies KaOS and Rei as being the most suitable among the examined frameworks, due to capabilities arising from their semantic web origins. Nevertheless, as the authors state *"Rei lacks a policy enforcement model and does not come with a graphical tool for policy specification and domain management. The main drawback of both is the fact that they are less scalable when the managed systems are large because complex ontology hierarchies need to be formed and reasoning about them is computationally expensive."*

Consistent with the results of these studies, in addition to the increased constraints imposed by the nature of military networks, studies conducted prior to this thesis [76] explored the capacity of semantic security policy frameworks to satisfy the underlying requirements. The results of such studies have been proven to satisfy the preconditions of the strategic domain, although a complete analysis within the realistic boundaries of SOA across the tactical domain remained unexplored.

1.6 Summary of Contributions

Seeking to address the research questions presented in section 1.3, in accordance to the background presented in section 1.4, and the delimited research frontiers identified in section 1.5, this thesis has resulted in the contributions outlined bellow.

1.6.1 List of publications

1. *1st Research Question:* Which are the operational and technical requirements for the attainment of fine-grained security goals within tactical SOA, under the constraints imposed by the characteristics of contemporary and future tactical operations?

    a) V. Gkioulos and S. D. Wolthusen, "Securing Tactical Service Oriented Architectures", 2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Paris, 2016, pp. 1-6.

    b) V. Gkioulos and S. D. Wolthusen, "Security Requirements for the Deployment of Services Across Tactical SOA", 7th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS), Warsaw, 2017, Springer, LNCS, volume 10446, pp. 115-127.

    c) V. Gkioulos and S. D. Wolthusen, "Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks", Norsk informasjonssikkerhetskonferanse - Norwegian Information Security Conference (NISK), Ålesund, 2015, pp. 109-120.

2. *2nd Research Question:* Which are the required architectural components and functionalities, for the enforcement of security controls within contemporary tactical SOA.

    a) V. Gkioulos and S. D. Wolthusen, "Security Infrastructure for Service Oriented Architectures at the Tactical Edge", 11th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), Torino, 2017, Springer, AISC, volume 611, pp. 310-322.

    b) V. Gkioulos, S. D. Wolthusen, A. Flizikowski, A. Stachowicz, D. Nogalski, K. Gleba and J. Sliwa, "Interoperability of Security and Quality of Service Policies Over Tactical SOA", 2016 IEEE Symposium Series on Computational Intelligence (SSCI), Athens, 2016, pp. 1-7.

3. *3rd Research Question:* How can a policy that is sufficiently expressive to allow the incorporation of discretionary access control, be formulated and implemented in a way that can satisfy the security requirements and constraints of tactical SOA?

    a) V. Gkioulos and S. D. Wolthusen, "A Security Policy Infrastructure for Tactical Service Oriented Architectures", Conference on

Security of Industrial-Control-and Cyber-Physical Systems (CyberICPS), Heraklion, 2017, Springer, LNCS, volume 10166, pp. 37-51.

b) V. Gkioulos and S. D. Wolthusen, "Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures", Advances in Network Systems. Advances in Intelligent Systems and Computing, Springer, AISC, volume 461, pp. 149-166.

c) V. Gkioulos and S. D. Wolthusen, "Efficient Security Policy Reconciliation in Tactical Service Oriented Architectures", 2nd International Conference on Future Network Systems and Security (FNSS), Paris, 2016, Springer, CCIS, volume 670, pp. 47-61.

4. *4th Research Question:* Given the results of the previous research questions, and a suitable reference architecture, can contemporary tactical networks support the deployment of security architectures developed according to the SOA paradigm?

   a) V. Gkioulos, E. Risthein and S. D. Wolthusen, "TACTICS: Validation of the Security Framework Developed for Tactical SOA", Journal of Information Security and Applications, 2017, Elsevier, volume 35, pp. 96-105.

1.6.1.1 Additional publications

The following publications resulted from parallel studies, which have been undertaken during the course of this thesis work.

1. V. Gkioulos, G. Wangen, S. Katsikas, G. Kavallieratos and P. Kotzanikolaou, "Security Awareness of the Digital Natives", Information 2017, 8(2), 42; doi:10.3390/info8020042, Special Issue Mobile Systems, Mobile Networks and Mobile Cloud: Security, Privacy and Digital Forensics.

2. V. Gkioulos, G. Wangen and S. Katsikas, "User Modeling Validation Over the Security Awareness of Digital Natives", Future Internet 2017, 9(3), 32; doi:10.3390/fi9030032, Special Issue Security and Privacy in Wireless and Mobile Networks.

3. V. Gkioulos, S. D. Wolthusen and A. Iossifides, "A Survey on the Security Vulnerabilities of Cellular Communication Systems (GSM-UMTS-LTE)", Norsk informasjonssikkerhetskonferanse - Norwegian Information Security Conference (NISK), Bergen, 2016, pp. 31-42.

1.6.2 List of major contributions

1. **1st Research Question**

   a) *Securing Tactical Service Oriented Architectures.*
   In this article we analyse the constraints of tactical SOA over the entire mission life cycle and derive a set of fine-grained security requirements, such that a TSPF based mechanism may optimally adjust to dynamic network conditions. Furthermore, we present the requisite characteristics of the developed security mechanisms, which are crucial for the real-time computation of policy decisions based on current situational knowledge. The contributions of this article can be summarised as:

      i. Analysis of constraints imposed over tactical SOA, arising from terminal and network characteristics.
      ii. Analysis of tactical mission phases, and the characteristics of the corresponding modes of network operation.
      These findings (i and ii) have been extracted according to initial network simulations, an extended literature review, and consultation with MoD (Ministry of Defence) representatives from the nations participating in TACTICS. This facilitated the explicit distinction between the nature of the strategic and tactical domains, incorporating both theoretical and practical data towards the:
      iii. Extraction of fine-grained security requirements for the protection of information, communication, data at rest, and processing for tactical SOA.
      iv. Identification of cross-layer information and meta-data domains, which can be utilised in order to enrich security policies, providing adaptability to dynamic network alterations during the mission life cycle.
      v. Identification of security operational domains, which are required to be supported and governed by a security architecture deployed within tactical SOA.

   b) *Security Requirements for the Deployment of Services Across Tactical SOA.*
   In this article we presented our analysis and results in respect of the secure deployment of services, as the means to process information and provide functionalities in tactical SOA. Analysing the interactions across the identified assets within pre-established scenarios, allowed the identification of potential transitive risk propagation paths. Focusing on the services as the main agent of such systems, operational and technical requirements have been

established towards the development of a secure tactical service infrastructure. The contributions of this article can be summarised as:

i. Identification and categorization of deployed assets within the context of tactical operations.
ii. Extraction of transitive threat model and analysis of transitive threat impact.
iii. Identification of operational requirements for service deployment within tactical SOA, and mapping them towards the security requirements presented in article 1.a.
iv. Extraction of technical requirements for the development of services within tactical SOA, with high criticality in respect of security.

c) *Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks.*
Through this article, the findings of our study regarding the constraints imposed by the nature of tactical SOA have been presented. These constraints have been translated into the corresponding functional requirements for the implementation of security mechanisms dedicated to tactical networks. Furthermore, the original architecture of the developed security policy framework has been suggested, incorporating the required components extracted by our earlier studies. Finally, an initial investigation has been undertaken towards utilising the expressive power of description logic and ontological constructs, for the sufficient realisation of the identified requirements. The contributions of this article can be summarised as:

i. Analysis of the tactical environment characteristics, which uniquely distinguish it from architectures developed for the strategic domain.
ii. Extraction of operational requirements for the developed security service oriented architecture.
iii. Analysis and initial modelling of the components that constitute the developed security policy framework.
iv. Investigation of the capacity of description logic and ontological constructs, to conceptualise and formally represent the developed security policy framework.

2. **2nd Research Question**

a) *Security Infrastructure for Service Oriented Architectures at the Tactical Edge.*

In this article we present the designed security service architecture, as developed in accordance to the requirements identified in our earlier studies. Each service is presented as an architectural element within the TACTICS TSI (Tactical Service Infrastructure), aiming to highlight the distinct functionalities of the security infrastructure towards the efficient enforcement of security controls at the tactical edge. The developed architecture provides configuration flexibility in a modular manner, while satisfying the defined requirements dynamically under varying network conditions. The contributions of this article can be summarised as:

i. Development of a security service oriented architecture dedicated to tactical SOA, in accordance to the identified requirements and existing models of confirmed performance.
ii. Analysis of the developed services, functionalities, interfaces and integrated policy decision extraction processes.

b) *Interoperability of Security and Quality of Service Policies Over Tactical SOA.*
In this article we propose a multi-domain policy-based decision subsystem supporting service delivery across tactical SOA, which relies on an online knowledge-based reasoning mechanism. We describe the characteristics of such a subsystem and show its benefits in relation to specific tactical requirements. Additionally, an insight has been provided over the utilised ontology and policy framework, focusing on the developed interoperability mechanism. The contributions of this article can be summarised as:

i. Investigation of constraints and requirements related to QoS and security operations.
ii. Investigation of benefits arising from a semi-unified decision subsystem for QoS and security.
iii. Analysis of core structural characteristics for the unified ontology and policy framework.
iv. Analysis of core operational characteristics and component for the unified interoperability architecture.

3. **3rd Research Question**

a) *A Security Policy Infrastructure for Tactical Service Oriented Architectures.*
In this article we have presented a security policy framework dedicated to tactical SOA, aiming to satisfy the identified requirements under the imposed constraints. The formal policy model has been presented and mapped to the developed core security services. Furthermore, the required steps for the formalisation

and deployment of policies have been described and analysed. The contributions of this article can be summarised as:

i. Definition of a formal policy model dedicated to tactical SOA.
ii. Mapping of the formal policy model to the security service architecture functionalities.
iii. Analysis of methodical process for the definition and deployment of security policies.

b) *Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures.*
In this article we analyse criteria and optimization goals for the a priori distribution and partitioning of security policies, ensuring the continuous support of the required capabilities, given the operational tasks of each deployed actor. Furthermore, a suitable mechanism has been suggested, accommodating the identified parameters, for the optimum partitioning and distribution of security policies within the mission preparation stage. The contributions of this article can be summarised as:

i. Identification of complexity inducing components in tactical ontological constructs.
ii. Classification and management analysis for tactical nodes.
iii. Analysis of dynamically evolving semantics within tactical ontological constructs.
iv. Development of a suitably adjusted policy partitioning mechanism for the mission preparation stage, according to constraint optimization techniques.

c) *Efficient Security Policy Reconciliation in Tactical Service Oriented Architectures.*
In this article we describe a mechanism that allows structured security policies to incorporate dynamic operational changes and efficiently reconcile across tactical SOA networks. This mechanism minimises the communication overhead compared to earlier work whilst maintaining policy integrity, thereby allowing security policies to adapt to resource and network constraints and other local knowledge alterations such as node compromises and blacklisting. The contributions of this article can be summarised as:

i. Identification and analysis of occurring divergences within the developed tactical security policies.
ii. Identification of the required components and functionalities for the reconciliation of the identified divergences.
iii. Development of a reconciliation mechanism according to the aforementioned analysis.

4. **4th Research Question**

    a) *TACTICS: Validation of the Security Framework Developed for Tactical SOA.*
    This article presents a comprehensive view of the security architecture developed within TACTICS, focusing on validating the elements that constitute the security framework according to our closing experimental results and field demonstrations. Furthermore, this article unifies the publicly available results of our security related studies, by highlighting how the distinct components presented earlier, interoperate towards the enforcement of security controls within tactical SOA. The contributions of this article can be summarised as:

        i. Validation of the overall security architecture in respect of a subset of required functionalities.

1.7 Limitations and recommendations for future work

This section includes a discussion over the limitations of the published articles and recommendations for future work. Accordingly, we seek to identify the extend of satisfactory fulfilment of the research questions by the publications that constitute this thesis, and propose research directions that can enhance the existing results.

1. **1st Research Question:** Currently the notion of tactical networks incorporates a variety of assets which operate as information sources, decision makers and effectors. Yet, the nature and characteristics of these assets are considerably dissimilar, given as an example that the combat management system of a naval vessel, and the wearable integrated war-fighter systems, are both components of contemporary battlefields. The studies performed within this thesis in respect of the 1st research question, analysed tactical networks as a unified ecosystem, comprising of land, air, and naval based components, where a consolidated SOA is required to be developed and deployed. Accordingly, the identified operational and technical requirements, along with the security goals and the environmental analysis, followed the paradigm of a unified tactical ecosystem. It is recommended that a taxonomy of asset classes is developed, categorising them both vertically (i.e. according to military services) and horizontally (i.e. according to characteristics and capabilities), seeking to identify fine-grained divergences through the application of information security risk management methods. This can highlight the potential for additional security management optimizations at the level of dedicated policy-based

management, without dissatisfying the requirement for a universal security architecture.

2. **2nd Research Question** The published articles present the results of our studies in respect of the required architectural components and functionalities, for the enforcement of security controls across contemporary SOA. The identified requirements as presented within the aforementioned publications, such as modularity of enforcement mechanisms, and cross platform deployment, have been satisfied and validated within the work presented in this thesis. Nevertheless, future work can focus on enabling additional capabilities, and further optimizations. Possible paths for future work can arise by seeking to optimally integrate the enforcement mechanisms as methods within the policy enforcement points. Additionally, the storage and reuse of extracted policy decisions at the mission execution stage, based on optimizations according to life-cycle and criticality measures, can be explored as a capability that can further improve the performance of the overall architecture. Finally, in respect of the designed QoS/ Security interoperability mechanism, future work can focus on the fine-grained analysis of the common policy framework, and architecturally in aspects related to deconflictation and the reduction of the negotiation cycles.

3. **3rd Research Question**

   The three articles that comprise our contribution in response to this research question, were focused on investigating the capacity of the solutions identified within research question 1, to satisfy the extracted requirements and constraints of tactical SOA. For this purpose a dedicated security policy framework has been developed in conjunction with the required extended capabilities. Future work can seek to further investigate how the syntactical and structural composition of ontological constructs affects reasoning time and complexity, aiming to further utilise the capabilities of the developed mechanisms and optimize policy specification at the mission preparation stage. Additionally, in respect of the partitioning of security policies during mission preparation, the integration of risk uncertainty as an additional variable, can be investigated as a solution for supporting nodes with even more constrained characteristics. Finally, given the extended analysis of potential policy divergences and required functionalities for addressing them, the developed algorithms for the formalization of the ordered functionality sets, can provide an additional path for future work, aiming to their optimization.

4. **4th Research Question** The results of the executed simulations, laboratory and field demonstrations, as presented in the corresponding

publication, have validated the capacity of tactical networks to support the deployment of security architectures developed according to the SOA paradigm. A subset of required functionalities have been thoroughly tested. Nevertheless, integration of additional capabilities and optimizations will require continuous validation and further analysis.

1.8 Conclusions

Securing constrained dynamic networks is a task intertwined with a multitude of challenges, arising both from the characteristics of the components that constitute the network, and the specific attributes of each application domain. During the course of our studies, tactical SOA have been examined as a representative application domain, towards the attainment of identified security goals, along capabilities delimited by domain specific operational requirements. Within this context, the focus of our studies has been targeted towards three research areas, as described in sections 1.1, 1.2, and 1.3.

Accordingly, the results of our studies highlighted the requirement for fine-grained security controls, towards the protection of communication, data at rest, and processing, which must dynamically accommodate both operational and functional requirements and constraints. Consequently, the incorporation of cross-layer information across the deployed security management subsystems becomes essential, allowing the detailed conceptualization of the operational environment , and by virtue of this, the fine-grained management and attainment of security related objectives. Furthermore, due to their integral role and overall reliance upon their efficient/ effective functionality, services and processes (either in the sense of service composition, or procedural processing) must be treated as distinct system entities along the phases of analysis, development, and system deployment. Finally, the developed security mechanisms must be adjusted not only to system specific attributes, but also to the characteristics of the deployment environment, and the anticipated operational conditions/ restrictions. This allows their adaptation to scenario specific constraints, and the accommodation of the required capabilities, maintaining the operability and enforceability of security control under severe operational constraints.

Furthermore, the suitable development and deployment of services within the TSSI, has been proven capable of fulfilling the long term objective of NEC/ NCW supporting tactical SOA. Within our studies, established functional components of contemporary security architectures (e.g. PEP, PDP), have been adjusted to the SOA paradigm, while complemented with additional services, functionalities and operational characteristics that accommodate the requirements of tactical SOA. As presented within our studies, and validated through the execution of simulations, laboratory experiments, and

field demonstrations, the SOA paradigm can be adjusted to the specifics of the tactical domain. Nevertheless, referring not only to security, but also on other aspects such as service delivery, session management, and QoS management, further optimizations and enhancements of the developed functionalities are required, prior to the deployment of fully functional systems on the field.

Finally, within our studies a suitable TSPF has been developed and tested, in accordance to the requirements and constraints identified earlier. An extensive initial state of the art review, highlighted policy-based management systems developed in accordance to semantic web technologies, as the most suitable mediator towards the attainment of the required functionalities. Accordingly, the focus of our studies has been on requirements specific to constrained and highly dynamic networks. Investigating and developing novel solutions, while complementing existing frameworks towards a structured multilayer policy-based management system, our studies focused on the specifics of the tactical domain. Accordingly, a structured formal policy model has been developed, seeking to accommodate the fine-grained semantics of the tactical environment, while suitable solutions have been investigated towards the fulfilment of well defined operational requirements (e.g. adaptation to dynamic network alterations, cross platform deployment and integration), under the identified network constrains.

Bibliography

[1] ISO/IEC 18384-1:2016(E): Information technology Reference Architecture for Service Oriented Architecture (SOA RA) Part 1: Terminology and concepts for SOA. 6

[2] ISO/IEC 18384-2:2016(E): Information technology Reference Architecture for Service Oriented Architecture (SOA RA) Part 2: Reference Architecture for SOA Solutions. 6

[3] ISO/IEC 18384-3:2016(E): Information technology Reference Architecture for Service Oriented Architecture (SOA RA) Part 3: Service Oriented Architecture ontology. 6

[4] ANDERS, E., RAYMOND, H., MAREK, M., ROLF, R., JEAN-YVES, S., MARC, S., OLE-ERIK, H., AND DOMINIQUE, G. Secure Service Oriented Architectures (SOA) Supporting NEC, RTO-TR-IST-061, ISBN 978-92-837-0069-2. Tech. rep., Research and Technology Organisation North Atlantic Treaty Organisation BP 25, F-92201 Neuilly-sur-Seine Cedex, France, 2009. 16

[5] ASCHENBRUCK, N., GERHARDS-PADILLA, E., AND MARTINI, P. A survey on mobility models for performance analysis in tactical mobile networks. *Journal of Telecommunications and Information Technology* (2008), 54–61. 11

[6] ASKOXYLAKIS, I., BENCSATH, B., BUTTYAN, L., DORA, L., SIRIS, V., AND TRAGANITIS, A. Cross-layer security and resilience in wireless mesh networks. 10

[7] BAR-NOY, A., CIRINCIONE, G., GOVINDAN, R., KRISHNAMURTHY, S., LAPORTA, T. F., MOHAPATRA, P., NEELY, M., AND YENER, A. Quality-of-information aware networking for tactical military networks. In *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (March 2011), pp. 2–7. 13, 83, 165

[8] BARZ, C. CoNSIS - Coalition Network for Secure Information Sharing. http://www.consis.info/, 2016. 16

[9] BARZ, C., AND QUINKERT, F. Advanced security gateways for heterogeneous tactical ad hoc networks. In *2015 International Conference on Military Communications and Information Systems (ICMCIS)* (May 2015), pp. 1–6. 15

[10] BECHHOFER, S., HARMELEN, F. V., HENDLER, J., HORROCKS, I., MCGUINNESS, D. L., PATEL-SCHNEIDER, P. F., AND STEIN, L. A. OWL Web Ontology Language Reference - W3C Recommendation - 10 February 2004. 11

[11] BLOEBAUM, H. T., JOHNSEN, T. F., LUND, K., AND BRANNSTEN, R. Core services recommendations and trends - RAPPORT 16/02484. Tech. rep., Norwegian Defence Research Establishment (FFI), December 2016. 17

[12] BLOEBAUM, T. H., JOHNSEN, F. T., BRANNSTEN, M. R., ALCARAZ-CALERO, J., WANG, Q., AND NIGHTINGALE, J. Recommendations for realizing soap publish/subscribe in tactical networks. In *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (May 2016), pp. 1–8. 14

[13] BORMANN, C., ERSUE, M., AND KERANEN, A. Terminology for Constrained-Node Networks. Status: INFORMATIONAL DOI: 10.17487/RFC7228, Internet Engineering Task Force (IETF), May 2014. 4

[14] BOUAM, S., AND BEN-OTHMAN, J. Data security in ad hoc networks using multipath routing. In *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.* (Sept 2003), vol. 2, pp. 1331–1335. 14

[15] BRUTCH, P., AND KO, C. Challenges in intrusion detection for wireless ad-hoc networks. In *2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings.* (Jan 2003), pp. 368–373. 14

[16] BU, S., YU, F. R., LIU, X. P., MASON, P., AND TANG, H. Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. *IEEE Transactions on Vehicular Technology 60*, 3 (March 2011), 1025–1036. 14

[17] BURBANK, J. L., CHIMENTO, P. F., HABERMAN, B. K., AND KASCH, W. T. Key challenges of military tactical networking and the elusive promise of manet technology. *IEEE Communications Magazine 44*, 11 (November 2006), 39–45. 13, 64, 83, 165

[18] CARVALHO, M. Security in mobile ad hoc networks. *IEEE Security Privacy 6*, 2 (March 2008), 72–75. 14

[19] CAYIRCI, E., AND RONG, C. *Security in wireless ad hoc and sensor networks*. John Wiley & Sons, 2008. 14

[20] CHENG, B. N., BLOCK, F. J., HAMILTON, B. R., RIPPLINGER, D., TIMMERMAN, C., VEYTSER, L., AND NARULA-TAM, A. Design considerations for next-generation airborne tactical networks. *IEEE Communications Magazine 52*, 5 (May 2014), 138–145. 12

[21] CHLAMTAC, I., CONTI, M., AND LIU, J. J.-N. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks 1*, 1 (2003), 13 – 64. 14

[22] CONDELL, M., LYNN, C., AND ZAO, J. Security Policy Specification Language. Tech. rep., Internet Engineering Task Force, 2000. 18

[23] CONTI, M., MASELLI, G., TURI, G., AND GIORDANO, S. Cross-layering in mobile ad hoc network design. *Computer 37*, 2 (Feb 2004), 48–51. 10

[24] CUPPENS, F., AND SAUREL, C. Specifying a security policy: a case study. In *Computer Security Foundations Workshop, 1996. Proceedings., 9th IEEE* (1996), IEEE, pp. 123–134. 18

[25] CURTIS-BLACK, A., WILLIG, A., AND GALSTER, M. A taxonomy for network policy description languages. In *2016 26th International Telecommunication Networks and Applications Conference (ITNAC)* (Dec 2016), pp. 159–165. 18

[26] DAMIANOU, N., BANDARA, A., SLOMAN, M., AND LUPU, E. A survey of policy specification approaches. *Department of Computing, Imperial College of Science Technology and Medicine, London 3* (2002), 142–156. 18, 42, 83

[27] DAMIANOU, N., DULAY, N., LUPU, E., AND SLOMAN, M. The Ponder policy specification language. *Policy 1* (2001), 18–38. 18, 19, 84, 143, 165, 215

[28] DUFLOS, S., DIAZ, G., GAY, V., AND HORLAIT, E. A comparative study of policy specification languages for secure distributed applications. In *International Workshop on Distributed Systems: Operations and Management* (2002), Springer, pp. 157–168. 18

[29] ELMASRY, G. F. A comparative review of commercial vs. tactical wireless networks. *IEEE Communications Magazine 48*, 10 (October 2010), 54–59. 12, 42, 83, 165

[30] ERSUE, M., ROMASCANU, D., AND SCHOENWAELDER, J. Management of Networks with Constrained Devices: Problem Statement and Requirements. Status: INFORMATIONAL DOI: 10.17487/RFC7547, Internet Engineering Task Force (IETF), May 2015. 4

[31] FU, Z., WU, S., HUANG, H., LOH, K., GONG, F., BALDINE, I., AND XU, C. Ipsec/vpn security policy: Correctness, conflict detection, and resolution. *Policies for Distributed Systems and Networks* (2001), 39–56. 18

[32] GARSTKA, J., ALBERTS, D., AND STEIN, F. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Command and Control Research Program (U.S.), 1999. 4

[33] GENESERETH, M. R., , AND NILSSON, N. J. Logical Foundations of Artificial Intelligence . Morgan Kaufmann, San Francisco (CA), 1987. Available from: `http://www.sciencedirect.com/science/article/pii/B978093461331650001X`. 10

[34] GERHARDS-PADILLA, E., ASCHENBRUCK, N., MARTINI, P., JAHNKE, M., AND TOLLE, J. Detecting black hole attacks in tactical manets using topology graphs. In *32nd IEEE Conference on Local Computer Networks (LCN 2007)* (Oct 2007), pp. 1043–1052. 14

[35] GOHDE, J., GRIFFIN, P., AND RICKENBACH, B. Tactical service-oriented architecture over wireless communications, 2007. Available from: `http://dx.doi.org/10.1117/12.721014`. 14

[36] GRUBER, T. A translational approach to portable ontologies. *Knowledge Acquisition 5*, 2 (1993), 199–220. 10

[37] GUARINO, N., OBERLE, D., AND STAAB, S. What is an ontology? In *Handbook on ontologies*. Springer, 2009, pp. 1–17. 10

[38] HAN, W., AND LEI, C. A survey on policy languages in network and security management. *Computer Networks 56*, 1 (2012), 477–489. 18

[39] HITCHENS, M., AND VARADHARAJAN, V. Tower: A language for role based access control. *Policies for Distributed Systems and Networks* (2001), 88–106. 18

[40] HOAGLAND, J. A., PANDEY, R., AND LEVITT, K. N. Security policy specification using a graphical approach. *arXiv preprint cs/9809124* (1998). 18

[41] JACOBS, S. Tactical network security. In *MILCOM 1999. IEEE Military Communications. Conference Proceedings (Cat. No.99CH36341)* (1999), vol. 1, pp. 651–655 vol.1. 14, 64

[42] JAJODIA, S., SAMARATI, P., AND SUBRAHMANIAN, V. S. A logical language for expressing authorizations. In *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)* (May 1997), pp. 31–42. 18

[43] JOHNSEN, F. T., FLATHAGEN, J., HAUGE, M., GJORVEN, E., MJELDE, T. M., AND LILLEVOLD, F. Cross-layer design and optimizations. Tech. Rep. FFI-rapport 2014/00985, FFI - Forsvarest forskningsinstitutt - Norwegian Defence Research Establishment, July 2014. 10

[44] KAGAL, L., FININ, T., AND JOSHI, A. A policy language for a pervasive computing environment. In *Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on* (2003), IEEE, pp. 63–74. 18, 19

[45] KAUL, V., MAKAYA, C., DAS, S., SHUR, D., AND SAMTANI, S. On the adaptation of commercial smartphones to tactical environments. In *2011 - MILCOM 2011 Military Communications Conference* (Nov 2011), pp. 2205–2210. 12

[46] KIDSTON, D., LI, L., TANG, H., AND MASON, P. Mitigating Security Threats in Tactical Networks. Tech. Rep. ADA584176, September 2010. 14, 64

[47] KONG, J., LUO, H., XU, K., GU, D. L., GERLA, M., AND LU, S. Adaptive security for multilevel ad hoc networks. *Wireless Communications and Mobile Computing 2*, 5 (2002), 533–547. Available from: http://dx.doi.org/10.1002/wcm.75. 14

[48] LACHARITE, Y., NGUYEN, D. Q., WANG, M., AND LAMONT, L. A trust-based security architecture for tactical manets. In *MILCOM 2008 - 2008 IEEE Military Communications Conference* (Nov 2008), pp. 1–7. 14

[49] LI, L., AND VIGNERON, P. Properties of Mobile Tactical Radio Networks on VHF Bands. Tech. Rep. ADA584166, September 2010. 12

[50] LOU, W., AND FANG, Y. *A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions*. Springer US, Boston, MA, 2004, pp. 319–364. Available from: http://dx.doi.org/10.1007/978-1-4613-0223-0_9. 14

[51] LOU, W., LIU, W., ZHANG, Y., AND FANG, Y. SPREAD: Improving network security by multipath routing in mobile ad hoc networks. *Wireless Networks 15*, 3 (2009), 279–294. Available from: http://dx.doi.org/10.1007/s11276-007-0039-4. 14

[52] MALOWIDZKI, M., DALECKI, T., BEREZINSKI, P., MAZUR, M., AND SKARZYNSKI, P. Adapting standard tactical applications for a military disruption-tolerant network. In *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (May 2016), pp. 1–5. 15, 214

[53] MAULE, R. W., AND LEWIS, W. C. Security for distributed soa at the tactical edge. In *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE* (Oct 2010), pp. 13–18. 15, 83, 165

[54] MAZZINI, A., STEFANELLI, C., TORTONESI, M., BENINCASA, G., AND SURI, N. Disservice: Network state monitoring and prediction for opportunistic information dissemination in tactical networks. In *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE* (Oct 2010), pp. 555–560. 13

[55] MOORE, B., ELLESSON, E., STRASSNER, J., AND WESTERINEN, A. Policy Core Information Model - RFC 3060. Tech. rep., The Internet Society - Network Working Group, 2001. 8, 19

[56] PHAN, T., HAN, J., SCHNEIDER, J. G., EBRINGER, T., AND ROGERS, T. A survey of policy-based management approaches for service oriented systems. In *19th Australian Conference on Software Engineering (aswec 2008)* (March 2008), pp. 392–401. 19

[57] REIDT, S., AND WOLTHUSEN, S. D. Efficient distribution of trust authority functions in tactical networks. In *2007 IEEE SMC Information Assurance and Security Workshop* (June 2007), pp. 84–91. 14

[58] SALEEM, A., AND KUMAR, N. Cross Layer Design Approach in Wireless Mobile ADHOC Network Architecture. *International Journal of Advanced Research in Computer and Communication Engineering 2*, 3 (March 2013), 1450–1457. 10

[59] SAUER, L., MASCHINO, M., MORROW, J., AND MAYHEW, M. Towards achieving cross domain information sharing in a soa-enabled environment using mils and mls technologies. In *MILCOM 2009 - 2009 IEEE Military Communications Conference* (Oct 2009), pp. 1–5. 15

[60] SCOTT, K. Disruption tolerant networking proxies for on-the-move tactical networks. In *MILCOM 2005 - 2005 IEEE Military Communications Conference* (Oct 2005), pp. 3226–3231 Vol. 5. 13

[61] SEIFERT, H., FRANKE, M., DIEFENBACH, A., AND SEVENICH, P. SOA in the CoNSIS coalition environment: Extending the WS-I Basic Profile for using SOA in a tactical environment. In *2012 Military Communications and Information Systems Conference (MCC)* (Oct 2012), pp. 1–6. 17, 214

[62] SHARMA, K., AND GHOSE, M. K. Cross Layer Security Framework for Wireless Sensor Networks. *International Journal of Security and Its Applications 5*, 1 (January 2011), 39–52. 10

[63] SIMANTA, S., PLAKOSH, D., AND MORRIS, E. Web services for handheld tactical systems. In *2011 IEEE International Systems Conference* (April 2011), pp. 115–122. 15

[64] SINGHAL, A., WINOGRAD, T., AND SCARFONE, K. Guide to Secure Web Services, Recommendations of the National Institute of Standards and Technology, Special Publication 800-95. Tech. rep., Computer Security Division, Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 - U.S. Department of Commerce, 2007. 17

[65] SIOUTIS, C. Introducing tactical to enterprise integration. In *2016 Military Communications and Information Systems Conference (MilCIS)* (Nov 2016), pp. 1–6. 13

[66] SLOMAN, M., AND LUPU, E. Policy specification for programmable networks. *Active Networks* (1999), CH355–CH355. 18

[67] SLOMAN, M., AND LUPU, E. Security and management policy specification. *IEEE Network 16*, 2 (Mar 2002), 10–19. 18, 42, 83

[68] SRIVASTAVA, V., AND MOTANI, M. Cross-layer design: a survey and the road ahead. *IEEE Communications Magazine 43*, 12 (Dec 2005), 112–119. 9, 123

[69] STERBENZ, J. P. G., KRISHNAN, R., HAIN, R. R., JACKSON, A. W., LEVIN, D., RAMANATHAN, R., AND ZAO, J. Survivable mobile wireless networks: Issues, challenges, and research directions. In *Proceedings of the 1st ACM Workshop on Wireless Security* (New York, NY, USA, 2002), WiSE '02, ACM, pp. 31–40. Available from: `http://doi.acm.org/10.1145/570681.570685`. 12

[70] SURI, N., BENINCASA, G., LENZI, R., TORTONESI, M., STEFANELLI, C., AND SADLER, L. Exploring value-of-information-based approaches to support effective communications in tactical networks. *IEEE Communications Magazine 53*, 10 (October 2015), 39–45. 13

[71] SURI, N., BENINCASA, G., TORTONESI, M., STEFANELLI, C., KOVACH, J., WINKLER, R., KOHLER, U. S. R., HANNA, J., POCHET, L., AND WATSON, S. Peer-to-peer communications for tactical environments: Observations, requirements, and experiences. *IEEE Communications Magazine 48*, 10 (October 2010), 60–69. 12

[72] SURI, N., MORELLI, A., KOVACH, J., SADLER, L., AND WINKLER, R. Agile computing middleware support for service-oriented computing over tactical networks. In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)* (May 2015), pp. 1–5. 16, 214

[73] SURI, N., REBESCHINI, M., BREEDY, M., CARVALHO, M., AND ARGUEDAS, M. Resource and service discovery in wireless ad-hoc networks with agile computing. In *MILCOM 2006 - 2006 IEEE Military Communications conference* (Oct 2006), pp. 1–7. 16

[74] TONTI, G., BRADSHAW, J., JEFFERS, R., MONTANARI, R., SURI, N., AND USZOK, A. Semantic web languages for policy representation and reasoning: A comparison of kaos, rei, and ponder. *The semantic web-ISWC 2003* (2003), 419–437. 18

[75] TOWNSEND, E. The 25-year history of service-oriented architecture. *URI: www. eriktownsend. com/white-papers/technology. Online* (2008). 6

[76] TRIVELLATO, D., ZANNONE, N., GLAUNDRUP, M., SKOWRONEK, J., AND ETALLE, S. A semantic security framework for systems of systems. *International journal of cooperative information systems 22*, 01 (2013), 1350004. 20, 84, 143, 165, 189, 190, 215

[77] USZOK, A., BRADSHAW, J., JEFFERS, R., SURI, N., HAYES, P., BREEDY, M., BUNCH, L., JOHNSON, M., KULKARNI, S., AND LOTT, J. Kaos policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement. In *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks* (June 2003), pp. 93–96. 18, 19, 84

[78] VARADHARAJAN, V., SHANKARAN, R., AND HITCHENS, M. Security for cluster based ad hoc networks. *Computer Communications 27*, 5 (2004), 488 – 501. Available from: `http://www.sciencedirect.com/science/article/pii/S014036640300286X`. 14

[79] VEDAMUTHU, A. S., ORCHARD, D., HIRSCH, F., AND HONDO, MARYANN YENDLURI, P. B. T. Y. U. Web Services Policy 1.5 - Framework. Tech. rep., World Wide Web Consortium (W3C), 2007. 19

[80] WANG, Y., CHEN, I. R., CHO, J. H., AND TSAI, J. J. P. Trust-based task assignment with multiobjective optimization in service-oriented ad hoc networks. *IEEE Transactions on Network and Service Management 14*, 1 (March 2017), 217–232. 15

[81] WATKINS, D., AND SCOTT, C. Methodology for evaluating the effectiveness of intrusion detection in tactical mobile ad-hoc networks. In *2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No.04TH8733)* (March 2004), vol. 1, pp. 622–627 Vol.1. 14

[82] WEI, C., LI, Y., AND LV, C. *A Cross-Layer Security Framework for Wireless Mesh Networks*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 107–114. Available from: http://dx.doi.org/10.1007/978-3-642-27323-0_14. 10

[83] WEI, Z., TANG, H., YU, F. R., WANG, M., AND MASON, P. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. *IEEE Transactions on Vehicular Technology 63*, 9 (Nov 2014), 4647–4658. 14

[84] WESTERINEN, A., SCHNIZLEIN, J., STRASSNER, J., SCHERLING, M., QUINN, B., HERZOG, S., HUYNH, A., CARLSON, M., PERRY, J., AND WALDBUSSER, S. Terminology for Policy-Based Management - RFC 3198. Status: INFORMATIONAL, The Internet Society - Network Working Group, 2001. 7

[85] WIES, R. Using a classification of management policies for policy specification and policy transformation. In *Integrated Network Management IV*. Springer, 1995, pp. 44–56. 17

[86] YI, P., WU, Y., ZOU, F., AND LIU, N. A survey on security in wireless mesh networks. *IETE Technical Review 27*, 1 (2010), 6–14. Available from: http://www.tandfonline.com/doi/abs/10.4103/0256-4602.58969. 14

[87] ZHOU, L., AND HAAS, Z. J. Securing ad hoc networks. *IEEE Network 13*, 6 (Nov 1999), 24–30. 14

Chapter 2

Article 1a: Securing Tactical Service Oriented Architectures

Securing Tactical Service Oriented Architectures

2016 International Conference on Security of Smart Cities, Industrial Control Systems and Communications (SSIC), Paris, 2016, pp. 1-6

Gkioulos, Vasileios Wolthusen, Stephen D.

Abstract

Service Oriented Architectures have been increasingly evaluated and applied within military networks. However, existing implementations tend to overlook the constraints of the tactical environment, generating unsuitable requirements of network resources. The ongoing TACTICS project aims to study these constraints and propose solutions suitably adjusted to the tactical ecosystem. Under this scope, the implementation of security architectures presents significant challenges and limitations. In this article we analyse the constraints of tactical SoA over the entire mission life cycle and derive a set of fine granularity security requirements, such that a security policy mechanism may optimally adjust to dynamic network conditions. Furthermore, we present the requisite characteristics of the developed security mechanisms, which are crucial for the real-time computation of policy decisions based on current situational knowledge.

2.1 Introduction

Current tactical infrastructures comprise of contemporary C2 and C4I systems of increasing complexity and heterogeneity. Yet, the transition towards NEC [1] and NCW [17, 2, 21], promoted the adaptation of SOA for the achievement of the required operational flexibility and dynamic adaptation, maintaining consistent transactions and information exchanges. Service oriented architectures provide established standards for applications over classical enterprise environments. Yet, the applicability over constraint wireless networks requires the establishment of suitable adaptation mechanisms.

Undertaken research across the fields of military operations [11, 7, 19], SOA [16, 15, 23, 13, 14] and security policy standards [6, 20, 22, 4], promoted

the adaptation of the SOA paradigm across the strategic domain, with applications also, to limited extend, into the tactical domain. Yet, the existing NATO C3 System Architecture Framework [18] focuses primarily on the strategic command echelons, without considering the various constraints imposed by the nature of the tactical environment (e.g. disruptions, mobility, congested or restricted networks). Furthermore, The German project RuDi, under the scope of security, aimed to the definition of protection services and applications, but did not consider functional constraints critical for the applicability of such architectures within the tactical domain, such as storage and computational limitations. Finally, the international project CoNSIS aimed to improve existing ESB (Enterprise Service Bus) mechanisms within rapidly evolving networks, without utilizing state of the art implementations for the definition of security policies with the use of ontological constructs.

The TACTICS project refers to an ongoing work, planned to be carried on until 2017. The security related aspects of the project include:

- Monitor and advice on security related aspects and requirements.
- Security of cross-layer network capabilities.
- Investigation of secure protocols and algorithms for robust distributed service storage, retrieval, and discovery.
- Investigation of secure, efficient and robust overlay routing with the incorporation of cross-layer information.
- Identification of lightweight and dynamic protection mechanisms.
- Identification of suitable information filtering, classification and provenance assurance mechanisms.
- Analysis and definition of robust and adaptable security policies for tactical SOA

Within this context [3], in our earlier studies, the constraints, functional requirements and formalization of ontologically defined security policies have been identified [8], followed by the analysis of corresponding distribution [10] and reconciliation mechanisms [9]. In this article our initial findings regarding the constraints and protection requirements of tactical SOA are identified. Furthermore, the operational modes of the implemented security mechanisms are presented and analysed in conjunction with the required elements of policy design.

2.2 Constraints of the Tactical Environment

Tactical networks have characteristics similar to Ad-Hoc and mesh networks, with additional constraints and requirements due to their military oriented nature. Increased information exchanges and intra/ inter node invocations, follow patterns dictated by mission specific requirements, tasks and phases. Yet, scarcity of resources and external parameters (e.g. environmental conditions, terrain, adversarial activities) impose sources of significant impact to the network performance and quality of service. The identified constraints can be categorised as terminal or network oriented.

Tactical terminals are of significant dissimilarity regarding both the serving platforms and their technical capabilities, extending to hand-held devices or sensors. Network performance and quality of service can be affected by terminal limitations referring to:

- Transmission/ Reception range
- Input/ Output limitations
- Power consumption
- Physical limitations
- Environmental conditions
- Interconnection capabilities
- Computational capacity

Furthermore, the identified network oriented constraints have been categorised as:

- **Transmission disruptions:** Due to radio range, interference (e.g. packet collisions, multipath transmission, jamming), physical obstacles, active attacks (e.g. wormhole, black-hole, denial of service)
- **Mobility:** Due to dynamic network configurations (Referring both to routing and IP/ ID planning and management), coalition operations, service delivery handover, multi-network affiliation.
- **Communication:** Due to scarcity of available radio resources (e.g. bandwidth, frequencies), protocols, and radio characteristics (e.g. packet error rate, jitter, delay)
- **Application layer:** Due to service delivery, discovery and registry management.

The challenge for securing tactical SOA rises by meeting the required protection goals (section 2.3), under the specific constraints and requirements of the tactical environment. Thus, suitable security policies must be designed and dynamically adapted to the environmental conditions, the characteristics of the protected services, and the existing QoS requirements or capabilities. [12].

Two distinct communication infrastructures are defined within the ecosystem of military communication networks. Standard SOA architectures can be utilised for the over-provisioned strategic domain, while the constrained nature of the tactical domain requires the use of distributed SOA. The strategic domain can provide continuous connectivity with the use of stable network infrastructure, while the tactical domain can only be assumed to offer intermittent and opportunistic connectivity through DTN. Due to these constraints the realization of security mechanisms within the tactical domain requires the adaptation of distributed SOA. Thus, the tactical domain requires the suitable exploitation of resources, in the limited timeframes where sufficient connectivity is available, in order to check, deploy or update the security mechanisms. A tactical operation is divided in the following phases:

1. Mission preparation: Executed at the strategic domain, prior to the operation, with no resource limitations. At this stage the security mechanisms will have no significant limitations on autonomy and processing power.

2. Mission execution: It is executed at the tactical domain and demands the periodic dynamic adaptation of the security functionalities over the current networks conditions. At this stage node mobility, intermittent connectivity, dynamic topologies and the node functional characteristics require disruption tolerant functionality of the deployed security mechanisms, maintaining consistency and autonomy.

3. Mission debrief: Executed at the strategic domain after the tactical operation, in order to synchronize, analyse and compile the operation reports and logs.

Within these stages the required security goals will have distinct levels of criticality, due to the dissimilar constraints and requirements of the strategic and tactical domains. Through the mission execution stage, where tactical SOA are deployed, two modes of operation are defined.

Continuous connectivity refers to a state where the defined service provider and the corresponding clients, retain sufficient connectivity for a time frame sufficient for the execution of a particular service/ functionality. In a

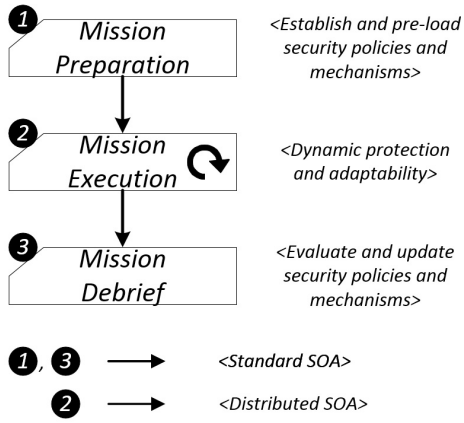

Figure 2.1: Phases of a tactical operation.

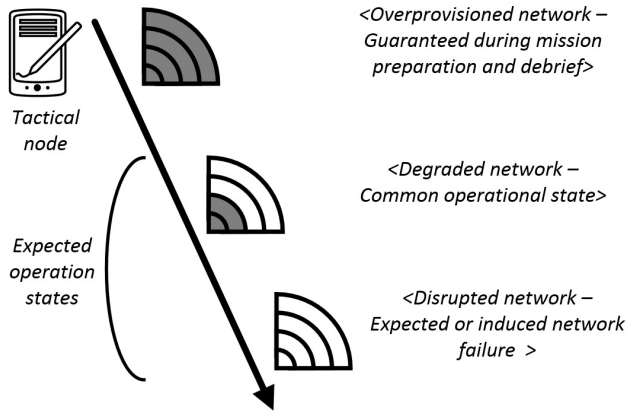

Figure 2.2: Network connectivity stages.

tactical network, nodes can maintain continuous connectivity when stationary and near communication infrastructure or while moving in a predicable manner, such as a convoy formation. In these scenarios the security infrastructure can utilize semi-centralized approaches in order to deploy and enforce policies, where the policy enforcement and decision points are assigned to the most suitable available node, based on an on-line evaluation of network resources and conditions, for a long period across the mission life-cycle.

Degraded operation occurs when network performance is compromised due to excessive resource consumption, physical barriers, malfunctioning

equipment, active attacks or mission specific functionalities. A network is considered to operate under degraded status when some of the required performance parameters falls out of the desirable and predefined limits. Such parameters may refer to connectivity, affecting the networks' QoS or service availability. For example, a service may partially fail when a set of subservices cannot be reached or executed. In this case, the service can still be invoked and accessed. Yet, it cannot provide the full set of required functionalities. Thus, degraded status refers to a state between continuous connectivity and disrupted communication, causing long delays due to packet loss, errors or disruptions. For this purpose, the deployed security policies must respond and dynamically adapt to the environmental conditions, but also support standalone and connectivity is-landed operation. This can be achieved by the distribution of dynamically adaptable security policies, across the deployed actors, based on the evaluation of their capabilities and mission requirements. Although mere replication is not sufficient, the main assumption of distributed security architectures is creating redundancy by having copies of access control mechanisms and policy databases on multiple nodes. Furthermore, the utilization of utility functions (e.g. mobility patterns, history of past encounters, social node characteristics) and the on-line evaluation of dynamic network attributes, can provide sufficient dynamism and adaptation of the security infrastructure, in order to maintain support of the defined security goals under degraded operation. Three types of degraded operation can be identified, namely:

1. Isolated: The node is disconnected from the network and can only make use of local services. Thus, external core and coalition services are unreachable.

2. Fragmented: The network is partitioned and the nodes reorganized. Core and coalition services can be available and opportunistic connections possible.

3. Is-landed: The network is operational without connection with the strategic domain.

2.3 Identified Security Requirements

Protecting tactical SOA requires the realization of generic protection goals, similar to those found in other systems, such as:

- Confidentiality
- Control
- Integrity
- Authenticity
- Availability
- Authentication
- Authorization
- Non Repudiation
- Utility
- Accountability
- Trust
- Traceability

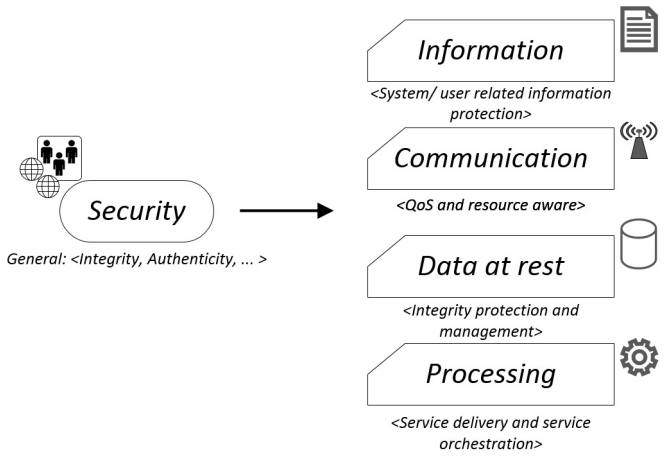

Figure 2.3: Outline of protection goal mapping.

Yet, the unique constraints and additional, or even mutually conflicting objectives, call for the establishment of robust and flexible multilayer security mechanisms. Furthermore, the prioritization of these goals must be dynamically adjusted over time to the specifics of each tactical operation. Thus, the realized security mechanisms must distinguish different components and phases of the tactical operation, by explicitly referring to information, communication, data at rest and processing. This classification allows the explicit protection of stored and transmitted information, in addition to the communication and processing as distinct assets of the tactical environment, within the inherently dynamic nature of SOA [24, 5]. These additional requirements, classified according to the aforementioned domains, are:

1. **Information**

    a) Information life cycle: Both information and processing mechanisms must be subjected to life cycle models, including mechanisms for purging a datum from a device. Furthermore, in the

case of encrypted information, this protection goal can be transformed into a key management problem, regarding the requirement for key storage and deletion, in order to ensure that no useful information can be retained.

b) Coalition environment considerations: The implemented security mechanisms must be able to add and remove entities across distinct trust layers. It can be applied on a per-mission basis, with the use of statistical or dynamic mapping.

c) Filtering: Information filtering mechanisms must be available within the security architecture, providing that information are subjected to suitable transformations, rendering them suitable for the expected set of recipients.

d) Environmental constraints: Information must be associated to ancillary attributes, regarding the circumstances it was processed or generated. This protection goal is required for the support of previously established requirements, such as authenticity, provenance and traceability.

e) Supporting information: Security policy decisions can be efficiently refined by the use of extended supporting information, which may arise from a variety of sources. Such information can be used for the validation, invalidation and corroboration of assertions and assumptions regarding the state of the tactical network.

2. **Communication**

a) Channel utilisation minimisation: Communications must minimise both the frequency and duration of information transmissions and requests. The purpose of this protection goal is focused on efficiency considerations, such as spectrum utilization and energy consumption. Furthermore, mission specific requirements are supported, such as EMCON (Emission Control) or constraint emission that prevents adversaries from gathering COMINT (Communication Intelligence) and ELINT (Electronic Signal Intelligence).

b) Channel utilization equalization: Channel utilisation should be equalised over time. This protection goal also prevents COMINT/ ELINT activities either on the communication protocol level, or on mission specific higher levels.

c) Channel reliability: A reliability metric must be provided mirroring the channels ability for message transmission. On the utilised multi-hop protocols, non reliable channels, bandwidth constraints and delays can prevent operations from completing with the

required quality of service parameters. The relevant characteristics will not necessarily be measurable or guaranteed in advance and must hence be estimated, where historical measurements are available.

d) Isolation policy: Isolated nodes must have an explicit policy in place for handling prolonged isolation from the mission network. Additionally, seeking to enforce re-establishment of communication links may leak COMINT/ ELINT and locality information. Thus, full isolation must be supported, including cases where reliable destruction of locally held cryptographic material is required.

e) Route information and preference: Communication channels must allow property recovery and constraint expressions. This protection goal aims to allow channel selection based on threat analysis and QoS intelligence.

f) Security service resource provisioning: The communication requirements for provisioning security services must inform minimum service level requirements, including contingency plans where these cannot be met.

g) Trust anchor: Nodes in a network must be equipped with a known good trust anchor for establishing communication with other nodes.

3. **Data at rest**

a) Mission Life Cycle Support of Security Mechanisms: Each processing unit must be capable of capturing mission parameters and modifying its behaviour according to the current state of the mission life-cycle.

4. **Processing**

a) Processing Integrity: Every processing unit must be capable of validating the integrity and authenticity of all code to be executed, by the use of appropriate assurance mechanisms.

b) Trustworthy initialization: Processing initialization must be supported by robust security mechanisms, for the validation of the processing node itself.

c) Dynamic Processing Integrity: Every processing unit must be capable of monitoring its own process integrity and to take mitigating measures on detection, by the use of control flow and data flow analysis mechanisms.

d) Security Service Assurance: Where security services are provided in an aggregate or layered form, the assurance offered by the aggregating service is necessarily the lowest offered by the constituent elements.

2.4 Elements of policy design

Security policies can be enriched with available cross layer information and meta-data regarding the operating status of various network elements, as presented at figure 2.4. Incorporating such information, can provide a refined security policy the decisions of which fulfil the defined security goals, while at the same time remain adaptable to the local and environmental conditions. In order to maintain the purity of the security policy, such cross layer information can be implemented with the use of ontological structures, and be categorised regarding their source and scope as:

1. Service domain: A tactical network must be able to provide some compulsory capabilities, including shared situational awareness, management of effects and fire support. This domain includes information, descriptive of the provided services. Service description may include static elements such as service type, classification, or the quality of the required input. On the contrary, the current status, possible providers or available service substitutions are some of the dynamic information, which can be utilised.

2. Information domain: The information generated by the users, services and infrastructure are of broad dissimilarity. These blocks of information differ in various characteristics, such as the nature of the included element (alerts, orders, tactical information), their source/ destination, type (data, voice, chat, signalling), size, generation frequency or their required quality, reliability and security features.

3. Network domain: This domain includes information used to form an understanding over the evolving topology of the network, including various topographic, social and mobility parameters. Some static information can be identified within this domain, such as the operational group that a node/ individual belongs too. Yet, since tactical networks consist of a highly versatile combination of ad-hoc and mesh networks, a wide variety of dynamic information may be incorporated, including a list of neighbouring nodes, the current location and the history of past encounters.

4. Radio domain: There is a wide variety of suitable radios for use within the tactical environment, including UHF (Ultra High Frequency), VHF (Very High Frequency), WLAN (Wireless Local Area Network) and

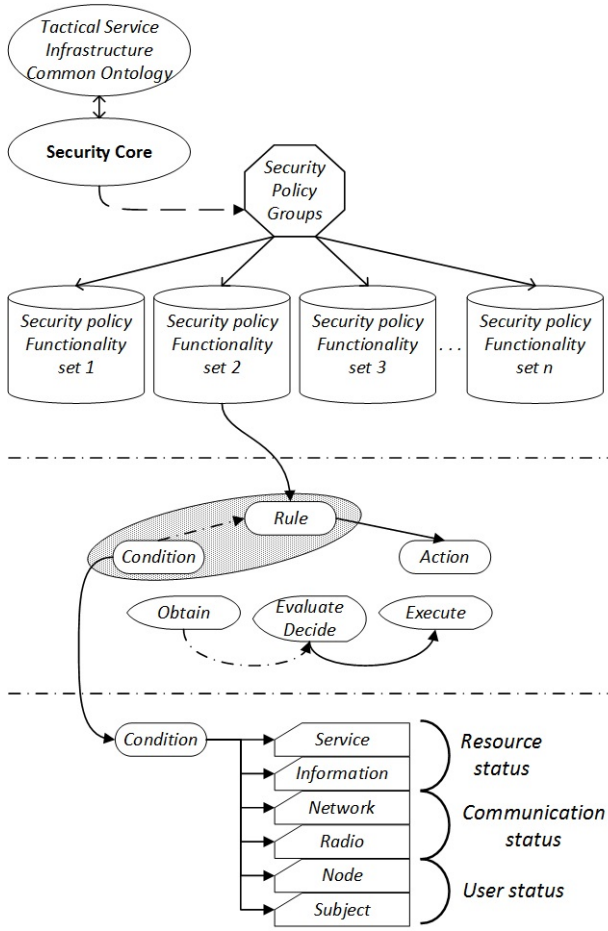

Figure 2.4: Incorporation of dynamic/ static cross-layer information across the security policy functionality/ decisions.

SatCom (Satellite Communications) based communication. The availability of such capabilities at any time within the lifetime of an operation, is crucial regarding network connectivity and service selection/ availability. The information which can be obtained may be static, such as the used band, Tx power and range, or highly dynamic such as available bandwidth. Additionally, monitoring of such radio information can be used, in order to achieve identification of active/ passive attacks and intrusion detection, leading to policy decisions of enhanced security.

5. Node domain: The involved assets within a tactical operation are of high heterogeneity. Thus, the used equipment is of high diversity with variable abilities and characteristics. This domain includes multiple static, such as the device code name, available communication protocols or available security mechanisms, and dynamic information, such as active operational feature (normal, low detection, low interception, anti-jam), trust level, resource availability and mobility history.

6. Subject domain: Additionally to the previously described information, each of the individuals that constitute a tactical group, has specific characteristics which determine the range of actions that can be undertaken within the network. The available information regarding each subject can include the rank, an identification, the current operational group and the overall role within the group.

Thus, each tactical node maintains a transmitter and a receiver status in respect to the security policy, which comprise of the aforementioned static and dynamic cross-layer information. Concurrently, a communication session between two nodes may require the evaluation of attributes across all the domains, while in SOA implementation the intermediate nodes may actively participate in the data manipulation and service execution, as presented in figure 2.5.

Such scenarios occur in SOA implementations, since a resource request can be served by one or many service providers. Thus, a service invocation can be distributed and served by multiple entities, in a variety of scenarios such as loops, direct links or fan out. Furthermore, mission specific requirements, resource constraints or environmental parameters may require the acquisition of immediate policy decisions in contrasts to the accuracy of the conditions that these decisions are based on. Such cases may include priority tactical alerts or messages with flash precedence. Thus, dedicated policy branches must be implemented, in order to dictate how these cases are treated by the security mechanisms.

Incorporating the aforementioned elements, a tactical security policy must represent and govern the interactions of entities across the distributed tactical ecosystem, achieving the realisation of the identified security goals. Thus, the security mechanisms must be able to gather information across various domains regarding the system's state and instantiate the security policy, which concurrently makes use of rich semantics in order to achieve the required functionalities. The required functionalities are supported by the identified security goals and have been categorised as:

1. Planning: It includes procedures that support the functionality of security mechanisms during the preparation phase of a tactical operation (e.g. pre-shared keys and inter-domain tuning for Communities Of Interest).

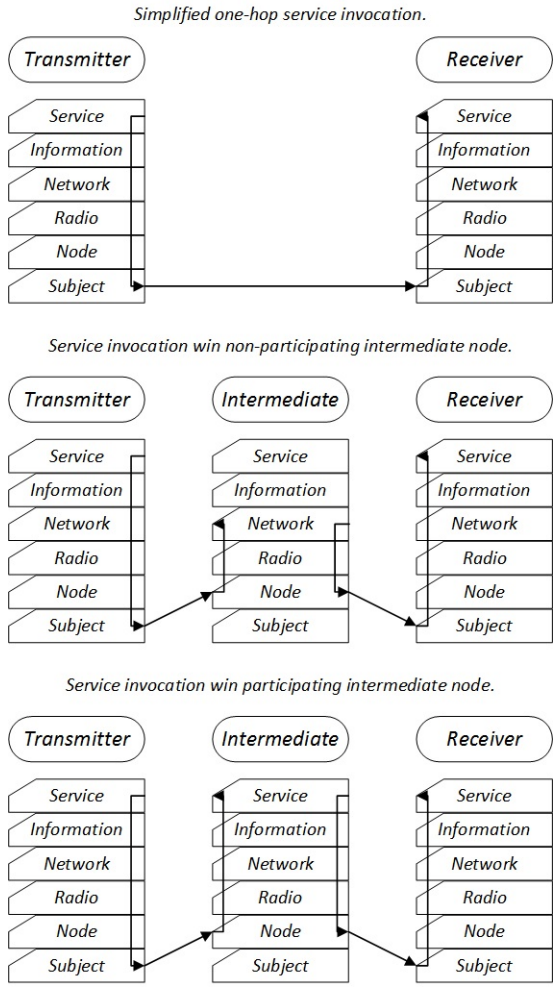

Figure 2.5: Policy rule / condition evaluation in simplified service invocation scenarios.

2. Protection: It includes tasks that actively imped undesirable activities that may compromise assets or disclose sensitive information (e.g. access control, information labelling and service security).

3. Detection: It includes rules in order to identify undesirable activities (e.g. cyber-attacks).

4. Diligence: It includes proactive measures to update the security mechanisms and policies (e.g. policy reconciliation or policy update).

5. Response: It includes processes that address violations after they have been detected (e.g. add services and nodes to a black list).

These internal policy functionalities may have different ways to implement their purposes across the various supported capabilities. Yet, the realization of robust but flexible governing rules, with the incorporation of dynamic cross-layer information, can provide the required on-line adaptation of the security mechanisms into the specifics of the occurring environmental alterations across a tactical operation.

2.5 Conclusions

Securing tactical SOA requires the realization of demanding protection requirements, for stored, transmitted and processed information. The implemented mechanisms for the realization of the defined requirements, must be able to support the identified functionalities under the constraints of the tactical environment, maintaining operability within the various tactical modes of operation. This can be achieved with the incorporation and on-line evaluation of existing cross-layer information, across the various network domains, within semantically enriched security policies. Concurrently, the defined security policies can dynamically adapt to the network alterations, adjusting the functionality of the security mechanism to the network attributes. The results of our studies presented in this article form the basis for our future work on the security of tactical SOA, within the scope of the ongoing project TACTICS.

Acknowledgments

The results described in this work were obtained as part of the EDA (European Defence Agency) project TACTICS (Tactical Service Oriented Architecture). The TACTICS project is jointly undertaken by Patria (FI), Thales Communications & Security (FR), Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE (DE), Thales Deutschland (DE), Leonardo (IT), Thales Italia (IT), NTNU: Norwegian University of Science and Technology (NO), ITTI (PL), Military Communication Institute (PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No.B0980.

Bibliography

[1] NATO Network Enabled Capability (NNEC), June 2014. Available from: http://www.act.nato.int/nnec. 42

[2] ALBERTS, D. S., AND HAYES, R. E. *Power to the Edge: Command and Control in the Information Age* . Information Age Transformation Series. Command and Control Research Portal, 2003. 42, 165

[3] ALOISIO, A., AUTILI, M., D'ANGELO, A., VIIDANOJA, A., LEGUAY, J., GINZLER, T., LAMPE, T., SPAGNOLO, L., WOLTHUSEN, S. D., FLIZIKOWSKI, A., AND SLIWA, J. TACTICS: TACTICal Service Oriented Architecture. *CoRR abs/1504.07578* (2015). Available from: http://arxiv.org/abs/1504.07578. 43, 63, 103, 121, 143, 154, 189, 191, 212

[4] BEN BRAHIM, M., CHAARI, T., BEN JEMAA, M., AND JMAIEL, M. Semantic Matching of WS-Security Policy Assertions. In *Service-Oriented Computing - ICSOC 2011 Workshops*, vol. 7221 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2012, pp. 114–130. Available from: http://dx.doi.org/10.1007/978-3-642-31875-7_13. 42, 84, 165

[5] BOSWORTH, S. *Computer Security Handbook*, 4th ed. John Wiley & Sons, Inc., New York, NY, USA, 2002. 48

[6] DAMIANOU, N., BANDARA, A., SLOMAN, M., AND LUPU, E. A survey of policy specification approaches. *Department of Computing, Imperial College of Science Technology and Medicine, London 3* (2002), 142–156. 18, 42, 83

[7] ELMASRY, G. F. A comparative review of commercial vs. tactical wireless networks. *IEEE Communications Magazine 48*, 10 (October 2010), 54–59. 12, 42, 83, 165

[8] GKIOULOS, V., AND WOLTHUSEN, S. D. Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks. *Norwegian Information Security Conference - NISK* (2015), 109–120. 43, 63, 103, 113, 122, 123, 143, 166, 168, 189, 191, 213, 218, 220

[9] GKIOULOS, V., AND WOLTHUSEN, S. D. Efficient security policy reconciliation in tactical service oriented architectures. In *International Conference on Future Network Systems and Security* (2016), Springer, pp. 47–61. 43, 63, 103, 113, 122, 123, 213, 223

[10] GKIOULOS, V., AND WOLTHUSEN, S. D. *Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures*. Springer International Publishing, Cham, 2017, pp. 149–166. Available from: http://dx.doi.org/10.1007/978-3-319-44354-6_9. 43, 63, 103, 113, 114, 122, 123, 143, 189, 191, 213, 218, 223

[11] HORNE, G., AND LEONARDI, M. *Maneuver Warfare Science 2001*. Marine Corps Combat Development Command, 2001. 42, 83, 165

[12] HUANG, D. Semantic descriptions ofweb services security constraints. In *Service-Oriented System Engineering, 2006. SOSE '06. Second IEEE International Workshop* (Oct 2006), pp. 81–84. 45

[13] IST-090 TASK GROUP. Service oriented architecture (SOA) challenges for real time and disadvantaged grid (IST-090). https://www.cso.nato.int/Activity_Meta.asp?ACT=1830, April 2014. 42, 83, 165

[14] IST-118 TASK GROUP. SOA recommendations for disadvantaged grids in the tactical domain (IST-118). https://www.cso.nato.int/ACTIVITY_META.asp?ACT=2293. 42, 83, 165

[15] JOHNSEN, F., BLOEBAUM, T., SCHENKELS, L., FISKE, R., VAN SELM, M., DE SORTIS, V., VAN DER ZANDEN, A., SLIWA, J., AND CABAN, P. SOA over disadvantaged grids experiment and demonstrator. In *Communications and Information Systems Conference (MCC), 2012 Military* (Oct 2012), pp. 1–8. 42, 83, 165, 214

[16] LUND, K., EGGEN, A., HADZIC, D., HAFSOE, T., AND JOHNSEN, F. Using web services to realize service oriented architecture in military communication networks. *Communications Magazine, IEEE 45*, 10 (October 2007), 47–53. 42, 65, 83, 165, 189

[17] MOFFAT, J. Adapting Modeling & Simulation for Network Enabled Operations. Tech. Rep. ADA555784, Defence Technical Information Center, 2011. 42, 165

[18] NATO CONSULTATION, COMMAND AND CONTROL BOARD BOARD (NC3B). C3 Taxonomy Perspective, Baseline 2.0, Enclosure 2 to 6300 TSC FCX 0010/TT-151521/Ser:NU, NC3B, November 2015. 43, 214, 220

[19] SHI, V. Evaluating the performability of tactical communications networks. *Vehicular Technology, IEEE Transactions on 53*, 1 (Jan 2004), 253–260. 42, 83, 165

[20] SLOMAN, M., AND LUPU, E. Security and management policy specification. *IEEE Network 16*, 2 (Mar 2002), 10–19. 18, 42, 83

[21] SMITH, E. A. *Complexity, Networking, and Effects-Based Approaches to Operations*. Center for Advanced Concepts and Technology, 2006. 42, 165

[22] STONE, G., LUNDY, B., AND XIE, G. Network policy languages: a survey and a new approach. *Network, IEEE 15*, 1 (Jan 2001), 10–21. 42, 83

[23] SURI, N. Dynamic Service-oriented Architectures for Tactical Edge Networks. In *Proceedings of the 4th Workshop on Emerging Web Services Technology* (New York, NY, USA, 2009), WEWST '09, ACM, pp. 3–10. Available from: `http://doi.acm.org/10.1145/1645406.1645408`. 42, 65, 83, 165

[24] UNITED KINGDOM CABINET OFFICE. HMG IA Standard No. 1: Technical Risk Assessment (Issue 3.51), CESG, UK, 2009. Tech. rep. 48

Chapter 3

Article 1b: Security Requirements for the Deployment of Services Across Tactical SOA

Security Requirements for the Deployment of Services Across Tactical SOA

7th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS), Warsaw, 2017, Springer, LNCS, volume 10446, pp. 115-127

Gkioulos, Vasileios Wolthusen, Stephen D.

Abstract

Service Oriented Architectures have been identified as a suitable mediator towards the attainment of the requirements imposed by modern warfare. Earlier studies focused primarily on the strategic domain, or the adaptation of such systems to the requirements of the tactical domain. Yet, the underlying constraints are significantly different between the two, with direct impact both on security and quality of service. In this article we approach the security aspect of tactical SOA, focusing on the specifics of the services while operating under the constrains and requirements of modern battlefields. Selected elements of our analysis within the project TACTICS are presented, as they have been utilized for the extraction of operational and technical requirements towards the development of a suitable tactical service infrastructure.

3.1 Introduction

Military operations are dependable on maintaining interoperability across the strategic and tactical domains. The strategic domain is commonly stationary or deployable, with over-provisioned infrastructure that supports elements such as headquarters, air combat command, intelligence command, mission control centres and medical treatment facilities. Contrary to that, the tactical domain is based on mobile infrastructures of ad-hoc nature supporting the communication requirements of the deployed units within the context of a tactical operation and across a given AoO. The military units

that must be served by the tactical SOA are commonly expected to be at levels equal or lower to a brigade, while tactical operations are commonly executed at the level of a company, platoon or section. Such operations present significant variations in terms of the AoO environment, expected mobility patterns, deployed assets, available resources, required services, information exchange models and mission sub-objectives. Yet, a tactical service oriented architecture must enable service provisioning across these variations, allowing the support of mission specific objectives according to established security and quality of service requirements.

Tactical networks bear some similarities to commercial MANET (Mobile ad-hoc) and mesh networks. Yet, due to their military orientation, they differentiate over a multitude of characteristics including the utilised technologies, their set of requirements and the imposed constraints. The introduction of the NEC and NCW paradigms within the domain of military networks, promoted the use of SOA for the attainment of these functionalities. However, the majority of existing SOA implementations have been developed focusing towards the enterprise domain, relying on infrastructures that can provide bandwidths of 100Mbits/ sec or more on a permanent basis. Contrary to that, the common capacity of tactical networks is less that 1Mbits/ sec, and they are deployed for short periods of time, while the common operational status is within the military VHF/ UHF bands. Additionally to the use of an error-prone and constraint communication medium, mission (e.g. enforcement of radio silence) and terminal (e.g. computational capacity, buffer size, battery) related constraints can also impede communications. Thus, both message and service delivery cannot be guaranteed.

Accordingly, our earlier studies [10, 8, 12, 9, 11, 29, 1, 7, 19] within the EDA project TACTICS focused on the investigation of suitable techniques, for the deployment of such mechanisms across contemporary C2 and C4I systems. TACTICS, aims to enable NCW and NEC, through the integration of information sources, effectors and services. Under this scope, the overarching objective is the definition, development and demonstration of a TSI architecture compatible with the realistic constraints and requirements of contemporary military operations. The developed TSI must allow existing tactical radio networks to participate in a core SOA infrastructure, while providing and consuming a set of required functional services. Additionally, the TSI must provide robust and efficient information transport within the tactical domain, but also to and from the strategic domain.

Maintaining a distinction between the information resources and the services (as the means to process information), is crucial for the attainment of security requirements in the environment of tactical SOA. Thus, in this article we focus on the services as the core element of TSI, presenting selected elements of our study, towards the extraction of corresponding operational and technical requirements for their development. The selected methodol-

ogy allowed the identification of assets, threats and security requirements, according to tactical scenarios, developed based on contemporary and future operational perspectives from the participating member states (non-disclosed). This allowed the extraction of operational and technical requirements, for the development of the TSI architecture with increased security related impact. Under this scope, risks have been assessed according to three evaluation criteria. These refer to the strategic value of the involved information assets, the criticality of the underlay information management services and the attainment of corresponding protection goals. The remainder of this paper is structured as follows. Section 3.2 introduces related work. Sections 3.3 and 3.4 present the assets, and direct or transitive threats that emerged from the analysis of the aforementioned scenarios. Finally, sections 3.5 and 3.6 highlight the identified operational and technical requirements for the development of services within tactical SOA.

3.2 Related Work

A multitude of earlier studies was focused on the investigation of security aspects related to commercial MANETS [23, 16, 22, 15, 24]. Yet, as described earlier, contemporary tactical ad-hoc networks present distinct sets of constraints and requirements, due to their unique operational and architectural characteristics. Thus, they must be distinctly investigated focusing primarily on the attainment of requirements imposed by tactical operations. Bass et al. [2] suggested a qualitative risk analysis method for complex network centric military operations. The authors focus on operations where information superiority is critical, analysing basic information assurance concepts and suggesting a risk management methodology for defence in depth. Kidston et al. [18] provided a generic study in respect to threat mitigation in tactical networks. The authors assessed the significant differences between commercial and tactical networks, supporting that, despite the similarities, security analysis and solutions cannot be considered a priori transitive within the two. Furthermore, the authors proposed a cross-layer security framework for the attainment of the corresponding security requirements.

Jacobs [13] provided a thorough examination of the adversary types, along with the corresponding threats they pose, towards a war-fighter information network. The author categorised the adversaries to spies, traitors, intelligent agents, information warriors and hostile soldiers, analysing each category in terms of expertise, access, backing and risk tolerance. Additionally, an overview of cryptographic methods has been provided, towards the mitigation of system vulnerabilities. Burbank et al. [4] evaluated the use of MANETs towards the realisation of the requirements of network centric warfare. Although the main focus of this study is not related to security as-

pects, the authors provide a thorough presentation of the requirements of tactical networks and the capabilities of current technologies towards their realisation.

Wang et al. [30] evaluated some of the security challenges and goals of tactical MANETS, suggesting a hierarchical security architecture for communication security management across large scale tactical ad-hoc networks. Additionally, Kidston et al. [17] presented a cross-layer architecture for network performance optimization, according to their analysis over system specific quality of service requirements. As presented earlier the requirements of NEC and NCW, promoted the use of service oriented architectures, for enabling such capabilities across tactical networks [20, 3, 28, 26, 6, 14, 27, 25, 5] . Yet, the field has not been studied in depth from the scope of security, or the operational assumptions do not coincide with the realistic constraints of the modern battlefield. Setting the services as the core element of tactical networks, within the constrained nature of the operational environments and infrastructures, impose a unique set of security requirements which we seek to identify and analyse within this study.

3.3 Asset Identification and Categorization

As stated earlier, the goal of this study was to define operational and technical requirements with security related impact, for the deployment of services across tactical SOA. Identifying and categorising the available assets, including the developed services, allowed the mapping and analysis of functional, transitive and symmetric interactions across them. This initial step is crucial for the identification of transitive risk propagation across the assets, and the analysis of mitigating measures from the perspective of the developed services.

AS-01, Personnel: According to the preservation of life requirement, the personnel involved in an operation is the asset of utmost criticality. This applies both to the decision making commanding officers, and, within the context of tactical operations, primarily to the network users deployed across the AoO.

AS-02, Information: Tactical SOA relies on the utilisation of cross-layer information for the establishment of the environmental context by defining objects, activities, and relations. In this context, information assets have been categorised as:

1. *AS-02.1, System specific:* Information that relate to the TSI architecture, such as:
    - Service interfaces
    - Service functionalities
    - Service input/ output formats

- Message/ packet processing chain
- Available cryptographic algorithms
- Service choreography diagrams
- Available overlay architectures
- Available routing protocols
- Security policy architecture
- QoS policy architecture

2. *AS-02.2, Mission specific/ Static:* Information that are established at the mission preparation stage and maintain absolute or high probability of remaining static through the mission execution stage, such as:

   - Deployed personnel (attributes)
   - Deployed functional services
   - Expected areas of operations
   - Deployed terminals (attributes)
   - Pre-shared cryptographic keys
   - Social/ hierarchical relationships among the deployed personnel and terminals
   - Objectives/ guidance information
   - Precedence/ Aggregation levels

3. *AS-02.3, Mission specific/ Dynamic:* Information generated by services, users and infrastructure during the mission execution stage, or are initialized during mission preparation, but are of dynamic nature, such as:

   - Blue/ red force tracking
   - Messaging services inputs/ outputs
   - Routing protocol data and statistics (available resources, link metrics)
   - Terminal/ service trust levels
   - Terminal resource metrics
   - Information dissemination paths
   - Service registry data and statistics

AS-3, Software: Software within a tactical SOA refers to the operating system and the deployed TSI architecture. Military systems commonly utilize commercial operating systems, such as Linux, Microsoft Windows or OS-X.

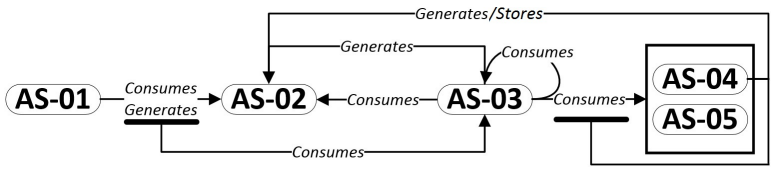

Figure 3.1: Interactions across the identified assets.

Yet, some special purpose domains are developed over operating systems specialised for military embedded systems. The TSI architecture refers to a set of core and functional services deployed across the tactical nodes in order to provide all the required mission and system-specific functionalities (e.g. unit positioning, medical evacuation alert, logging, session management, access control, information filtering/ labelling).
AS-4, Hardware: Hardware resources refer to the deployed terminals. It must be noted that within tactical networks highly diverse platforms are deployed, referring to ground, air, naval, deployed unmanned and satellite communications. Despite the diversity of these platforms in terms of capabilities, constraints, requirements and mobility, interoperability must be guaranteed for the support of the required functionalities.
AS-5, Network: Network resources are a critical asset within the constrained environment of tactical networks, since they directly affect the aforementioned elements through the information dissemination, service choreography and resource allocation processes. In that sense network resources refer not only to the available bandwidth, but also to a variety of other elements that may effect service delivery, such as computational capacity, battery level, packet queue size, memory size and radio range.

Figure 3.1 presents the model of interactions across the identified assets, that has been developed and used during the next steps of our analysis. Software/ Services (AS-03) are consumed by other services, and by the process of Personnel (AS-01) consuming or generating Information (AS-02). Furthermore, Service consumption can generate and consume Information, but also consumes Hardware (AS-04) and Network (AS-05) resources (which as a process also generates information).

An example of how the model has been used in the next steps of our analysis (in conjunction with the identified threats and requirements), can be extracted by the used scenarios as follows: The team leader of a section (AS-01) generates a medical evacuation alert message (AS-02), with the use of the MEDEVAC functional service (AS-03). In this scenario, the TSI must be developed according to technical specifications that allow the satisfaction of security requirements not only across the direct action path (e.g encryption and integrity protection of the MEDEVAC request), but also on potential

transitive paths, such as:

- Information leakage through the transitive consumption of other services (e.g. Distributed service registry, QoS Handler-Through the message prioritization process).
- Transitive Denial of Service attacks, if the consumption of the MEDEVAC functional service is dependable on the consumption of other (AS-03, AS-04, AS-05) assets.
- Information leakage through the consumption of AS-04 and AS-05 assets, for the prioritized routing of the MEDEVAC alert.

3.4 Analysis of Transitive Threat Impact for Tactical SOA

As presented earlier, the threats imposed to commercial and tactical networks have been thoroughly analysed in existing bibliography. Yet, for the purpose of this study it was critical to identify transitive relationships, in order to define technical requirements that could minimize security related risks. The selected basis of our analysis was the ENISA (European Union Agency for Network and Information Security) threat taxonomy [21]. Thus, filtering threats related to SOA across tactical environments, and identifying the affected assets in conjunction with the model presented in section 3.3, allowed the mapping of transitive impact propagation. The identified interactions can be seen in table 3.1, where Potential Threat Sources (PS), Direct Impact (DI), High Transitive Impact (HTI) and Low Transitive Impact (LTI) of threats, are presented.

Threat	**AS-01**	**AS-02**	**AS-03**	**AS-04**	**AS-05**	**External**
Lack of resources						
Lack of network capacity	PS/ LTI	HTI	PS/ HTI	LTI	PS/ DI	PS
Lack of processing power	PS/ LTI	HTI	PS/ DI	PS/ LTI	LTI	PS
Lack of storage capacity	PS/ HTI	DI	PS/ HTI	PS/ LTI	LTI	PS
Physical damage						
Destruction of equipment due to enemy activity	LTI	PS/ HTI	LTI	DI	HTI	PS

Destruction of equipment due to accidents or misuse	PS/ LTI	HTI	LTI	DI	HTI	
Loss of equipment possession	PS/ LTI	HTI	LTI	DI	LTI	PS
Failures						
Equipment failures - performance degradation (due to exposure to environmental conditions, hazardous materials, and operational conditions)	LTI	HTI	HTI	PS/ DI	LTI	PS
Software failures - performance degradation	HTI	LTI	PS/ DI	LTI	LTI	PS
Loss of stored information	PS/ HTI	DI	PS/ HTI	PS/ LTI	LTI	PS
Unintentional leakage of information in transit	HTI	DI	PS/ LTI	LTI	PS/ LTI	
Unauthorized/ Malicious actions						
Misuse of services	PS/ HTI	HTI	PS/ DI	LTI	LTI	
Misuse of hardware resources	PS/ HTI	LTI	PS/ HTI	DI	LTI	
Misuse of information	PS/ HTI	DI	PS/ HTI	LTI	LTI	
Misuse of network resources	PS/ HTI	LTI	PS/ HTI	LTI	DI	
Intentional disclosure of information	PS/ HTI	DI	PS/ HTI	LTI	LTI	
Incorporation of untrustworthy information	PS/ DI	HTI	PS/ DI	LTI	LTI	PS

Incorporation of malicious software (trojans, worms, viruses, bots, cracks, malware)	PS/ LTI	DI	PS/ DI	HTI	HTI	PS
Tampering with hardware resources	PS/ HTI	LTI	PS/ HTI	DI	LTI	PS
Tampering with software	PS/ HTI	HTI	PS/ DI	LTI	LTI	PS
Tampering with the network configuration	PS/ HTI	LTI	PS/ HTI	LTI	DI	PS
Social engineering	PS/ DI	DI	HTI	LTI	LTI	PS
Active attacks (flooding, Wormhole, Black hole, Rushing, Byzantine, Replay, Snooping, Fabrication, Denial of Service, Sinkhole, Man in the middle)	LTI	HTI	HTI	LTI	DI	PS
Passive attacks (traffic analysis, eavesdropping, monitoring)	LTI	HTI	HTI	LTI	DI	PS

Table 3.1: Transitive threat impact analysis for tactical SOA

An example of the scenarios used for this analysis can be extracted in respect to the ”Loss of stored information” threat. Internal sources of the threat are identified in AS-01 (misuse), AS-03 (software failure), and AS-04 (equipment failure). The direct impact is located in the lost information itself, while high transitive impact is traced at the assets consuming information (AS-01 and AS-03). Yet, low transitive impact can be traced to AS-04 and AS-05, since recapturing (or requesting retransmission), and reprocessing the lost information, will require the consumption of hardware and network resources in an already constrained network.

3.5 Identified Operational Requirements

Setting the services as the core network element instead of the radio links, imposes a unique set of requirements and vulnerabilities, that necessitate the incorporation of additional elements into the security paradigm of currently developed tactical architectures. In this section we aim to filter and analyse these elements that are specific to the service architecture and require the development of specialized controls or the suitable adaptation of the existing. Within the TSI, the deployed services obtain the role of network entities. In this sense, the available core and functional services must be treated not only as network resources that can be invoked by the users, but also as agents that can consume resources on their own right, such as bandwidth and other services.

Consequently, in this section we attempt a mapping of the functional requirements that emerged from our study, for the mitigation of the aforementioned threats, to well established and generic security requirements. This approach has been selected because thorough technical details of existing (such as those deployed at the strategic domain) or currently developed (aiming at the tactical domain, such as TACTICS TSI) military SOA, have not or can not be fully disclosed. It must be noted that approaching this topic from the perspective of services, does not exclude but is complementary to generic and information centric security requirements, as described earlier [10], while transitive dependencies also apply.

1. ***Availability:*** It does not only refer to information, but also the means to process these (meaning the deployed services), which must be available at the time they are required directly or transitively. Availability of information is generally understood in the sense of timeliness, which does not necessarily imply any particular speed of processing, but rather depends on the specification of a deadline. If no such deadline exists, the information must be available on demand, which may be considered a stronger requirement. For code and services, the goal of availability formulates a metric identifying the ability to process information and provide functionalities. For realistic tactical systems, availability is closely related to reliability and is often expressed as a probabilistic metric. In reliability theory, availability expresses the degree to which a system is in a specified operable and committable state during a mission, when it is called for, at an unknown (modelled as random) time. This fraction is often described as a mission capable rate (0 to 1).

2. ***Confidentiality:*** A service must not disclose information to unauthorised entities (including other services) allowing the deduction of its state. This does not explicitly establish confidentiality between prin-

cipals or services. Depending on the required granularity this may be achieved in the simplest case (however approximately) through access control mechanisms, but otherwise may require formulation over explicit information flows. We also note that information flows under non-deductibility are not limited to the deliberate exchange of information. As an example consider the use of radio frequencies which allows the observation of the fact that services communicate in a transitive manner, regardless of encryption or even traffic flow confidentiality. Similarly the use of a name service or service registry that is itself not kept confidential can allow the deduction of information regarding the internal state of the principal.

3. ***Control:*** Services must not relinquish possession of protected functionalities. This implies protection against tampering or the possibility of tampering within transitive or delegated service invocations. Such capabilities, including service substitution, are fundamentally required within tactical SOA. Yet, at each step of such invocation links, control must be maintained and reassured. Applying the notion of trust within this context, operations on information must only be performed if the service performing the operation can be believed to act in the interest of the service providing the data to be processed. In a more generic but equally significant approach, a service must be capable of initiating processing in a trusted state.

4. ***Integrity:*** The TSI must not allow information flows that may have been subject to modification by services at different levels of integrity than the originating principal. This is realised typically at different levels for data and services. For data, detecting whether any modification has occurred, and possibly the originating service of such modification, is a necessary component. Particularly for services, integrity can be shown at the level of identity, but as data may also be subjected to transformations either at the syntactical or even at the semantic level. This requires a clear understanding of metrics other than non-modification. Additionally, integrity may be considered as axiomatic or be represented by trust in a service, modelled explicitly either dynamically or statically. We note that integrity may be called into question when modification is possible rather than on demonstrating that it has occurred in actual fact. Furthermore, modifications must also map omission or suppression of information, rather than only differences between a received or stored copy of information and the original.

5. ***Authorisation:*** All service functionalities on or affecting protected information (direct, transitive or delegated service invocations) must be subjected to authorisation. This is an indirect prerequisite for accountability and information-related protection. It must be noted that infor-

mation flows and modifications may arise from local state change or previous and subsequent operations, requiring explicit consideration of such processing as part of the set of operations to be controlled.

6. ***Authenticity:*** Authenticity is a property that may again refer to information and services, and must not be confused with authentication, since it refers to obtaining proof or a relative metric to verify a claim either of origin or, more generally, of the provenance of a datum after processing. Authenticity can be proven ephemerally, but may also need to be verified after longer time periods have elapsed. In the former case, the proof or measure of authenticity exists for the duration of an interaction among services, whilst in the latter the proof or measurement must be stored or transported, and is itself the subject of protection. Where authenticity is to be shown over longer time periods, the notion of time or ordering must typically be included explicitly since violations of integrity of a datum or services operating on data may invalidate authenticity, or give rise to claims that data is not authentic.

7. ***Authentication:*** All information processing entities must be uniquely identified and authenticated. This is primarily required for accountability, but is also implicitly required in confidentiality and integrity protection mechanisms for information at the processing level.

8. ***Traceability and Non-repudiation:*** An unbroken chain must be retained documenting the provenance and transfer of information across all services, ensuring the inability of a principal to deny that a datum was generated, transferred or modified. The above can also be formulated positively in terms of requiring a service that provides proof of the integrity and origin of data, including the authenticity of this assertion with high assurance, where the integrity and authenticity must be possible to maintain without the cooperation of the principal whose datum is the subject of the non-repudiation proof. This is largely supported by integrity and authenticity assurance mechanisms, but requires additional information to be retained for each service involved in an information flow.

3.6 Identified Technical Requirements

The presented results of our theoretical analysis, allowed the identification of technical requirements, towards the architectural development stage of TACTICS. The identified requirements of high criticality for the mitigation of the aforementioned threats include:

1. Service definition according to standard formats, (e.g. XSD, WADL, WSDL) ensuring interoperability with the existing subsystems deployed within the strategic domain, and coalition operations.

2. Any implemented service invocation processes must support existing protocols, (e.g. SOAP, WSIF) ensuring interoperability with the existing subsystems deployed within the strategic domain, and coalition operations.

3. End-to-end dynamic service discovery and delivery must be supported across multiple domains.

4. Edge proxy functionality must be supported, in order to allow suitable and secure translation of messages and services.

5. Support a variety of message exchange schemes (anycast, broadcast, multicast, unicast) for dissemination of policy critical updates and service management/ invocation.

6. A distributed and best-effort updated service registry/ repository must be provided, in order to enhance service availability.

    - During service discovery, a consumer must be able to identify all the reachable services/ providers according to the defined security policy privileges.

7. Support of a dynamic and capable of preconfiguring publish/ subscribe exchange pattern.

8. Support of store and forward functionality.

9. Support of bandwidth reservation functionality.

10. Service substitution and delegation must be conditionally supported, not only within the same or neighbouring nodes, but also within allied forces.

    - This also applies for the security services including policy mechanisms.

11. The service discovery mechanism functionalities are independent of other core services and, within the TSI, constrained only by the security policy.

    - Externally, the service providers available resources must also be taken into account.

12. Required services and policies can be added or updated on-line, during the mission execution stage, given that the needed resources become available.

    - This should also be feasible using an unmanned operational node (e.g. UAV-Unmanned Aerial Vehicle)

13. Suitable mechanisms must be established in order to allow message prioritization both for system and mission specific messages. (e.g. security policy updates, dynamic attribute dissemination (trust levels), mission alerts).

    - Similarly, prioritization in congested environments must be allowed for the exposure of high criticality services.

14. The TSI supports a variety of overlay/ underlay routing protocols, in order to allow adjustments according to user mobility and disruptions, utilising and/ or maintaining multiple routes.

15. Security management and service protection is established at multiple levels and variable granularity within the SOA stack

16. The TSI can include a variety of core services, which are deployed across the tactical nodes at the mission preparation stage, according to node capabilities and mission requirements.

    - The minimum set and most lightweight versions of core services deployed in a tactical node must allow service discovery, message exchange and security. This would allow the stand alone operation of the node within is-landed or heavily congested environments.

17. Service dedicated access control, integrity protection, confidentiality, provenance assurance and trust management mechanisms are established within the security policy, as discrete network entities, as presented earlier.

18. Service features are evaluated and adapted dynamically to network and node resources, as well as user requirements, according to service performance indicators and SQM (Service Quality Management).

3.7 Conclusions

The constraints of tactical networks impose significant limitations to the realization of suitable SOA based solutions. Overcoming these limitations, while maintaining the enforcement of security requirements for the protection of the deployed assets is a critical task. In this article we presented our

analysis and results in respect to the secure deployment of services, as the means to process information and provide functionalities in tactical SOA. Analysing the interactions across the identified assets within pre-established scenarios, allowed the identification of potential transitive risk propagation paths. Focusing on the services as the main agent of such systems, operational and technical requirements have been established towards the development of a secure tactical service infrastructure. It must be noted again that approaching this topic from the perspective of services, must be enforced as complementary to generic and information centric security requirements, as described in our earlier studies.

Acknowledgments

The results described in this work were obtained as part of the European Defence Agency project TACTICS. The project is jointly undertaken by ITTI (PL), MCI (PL), Patria (FI), Thales Communications & Security (FR), FKIE (DE), Thales Deutschland (DE), Leonardo (IT), Thales Italia (IT), NTNU (NO), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980.

Bibliography

[1] ALOISIO, A., AUTILI, M., D'ANGELO, A., VIIDANOJA, A., LEGUAY, J., GINZLER, T., LAMPE, T., SPAGNOLO, L., WOLTHUSEN, S. D., FLIZIKOWSKI, A., AND SLIWA, J. TACTICS: TACTICal Service Oriented Architecture. *CoRR abs/1504.07578* (2015). Available from: `http://arxiv.org/abs/1504.07578`. 43, 63, 103, 121, 143, 154, 189, 191, 212

[2] BASS, T., AND ROBICHAUX, R. Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations. In *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE* (2001), vol. 1, IEEE, pp. 64–70. 64

[3] BIRMAN, K., HILLMAN, R., AND PLEISCH, S. Building net-centric military applications over service oriented architectures, 2005. Available from: `http://dx.doi.org/10.1117/12.605149`. 65

[4] BURBANK, J. L., CHIMENTO, P. F., HABERMAN, B. K., AND KASCH, W. T. Key challenges of military tactical networking and the elusive promise of manet technology. *IEEE Communications Magazine 44*, 11 (November 2006), 39–45. 13, 64, 83, 165

[5] CANDOLIN, C. A security framework for service oriented architectures. In *MILCOM 2007 - IEEE Military Communications Conference* (Oct 2007), pp. 1–6. 65

[6] CROOM JR, C. E. Service-oriented architectures in net-centric operations. Tech. rep., Defence Information Systems Agency ARLINGTON VA, 2006. 65

[7] DIEFENBACH, A., GINZLER, T., MCLAUGHLIN, S., SLIWA, J., LAMPE, T. A., AND PRASSE, C. Tactics tsi architecture: A european reference architecture for tactical soa. In *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (May 2016), pp. 1–8. 63, 103, 121, 144, 155, 218

[8] GKIOULOS, V., AND WOLTHUSEN, S. D. Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks. *Norwegian Information Security Conference - NISK* (2015), 109–120. 43, 63, 103, 113, 122, 123, 143, 166, 168, 189, 191, 213, 218, 220

[9] GKIOULOS, V., AND WOLTHUSEN, S. D. Efficient security policy reconciliation in tactical service oriented architectures. In *International Conference on Future Network Systems and Security* (2016), Springer, pp. 47–61. 43, 63, 103, 113, 122, 123, 213, 223

[10] GKIOULOS, V., AND WOLTHUSEN, S. D. Securing tactical service oriented architectures. In *2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)* (July 2016), pp. 1–6. 63, 71, 103, 113, 122, 123, 143, 154, 157, 189, 191, 213, 218, 220

[11] GKIOULOS, V., AND WOLTHUSEN, S. D. A security policy infrastructure for tactical service oriented architectures. In *Conference on Security of Industrial-Control-and Cyber-Physical Systems* (2016), Springer, pp. 37–51. 63, 103, 104, 113, 122, 123, 213, 218, 220, 222

[12] GKIOULOS, V., AND WOLTHUSEN, S. D. *Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures*. Springer International Publishing, Cham, 2017, pp. 149–166. Available from: http://dx.doi.org/10.1007/978-3-319-44354-6_9. 43, 63, 103, 113, 114, 122, 123, 143, 189, 191, 213, 218, 223

[13] JACOBS, S. Tactical network security. In *MILCOM 1999. IEEE Military Communications. Conference Proceedings (Cat. No.99CH36341)* (1999), vol. 1, pp. 651–655 vol.1. 14, 64

[14] JOHNSEN, F. T., FLATHAGEN, J., AND HAFSE, T. Pervasive service discovery across heterogeneous tactical networks. In *MILCOM 2009 - 2009 IEEE Military Communications Conference* (Oct 2009), pp. 1–8. 65

[15] KANNAMMAL, A., AND ROY, S. S. Survey on secure routing in mobile ad hoc networks. In *2016 International Conference on Advances in Human Machine Interaction (HMI)* (March 2016), pp. 1–7. 64

[16] KAUSER, S. H., AND KUMAR, P. A. Manet: Services, parameters, applications, attacks & challenges. 64

[17] KIDSTON, D., AND LI, L. Management through cross-layer design in mobile tactical networks. In *2010 IEEE Network Operations and Management Symposium - NOMS 2010* (April 2010), pp. 890–893. 65

[18] KIDSTON, D., LI, L., TANG, H., AND MASON, P. Mitigating Security Threats in Tactical Networks. Tech. Rep. ADA584176, September 2010. 14, 64

[19] LOPES, R. R. F., AND WOLTHUSEN, S. D. Distributed security policies for service-oriented architectures over tactical networks. In *MILCOM 2015 - 2015 IEEE Military Communications Conference* (Oct 2015), pp. 1548–1553. 63

[20] LUND, K., EGGEN, A., HADZIC, D., HAFSOE, T., AND JOHNSEN, F. Using web services to realize service oriented architecture in military communication networks. *Communications Magazine, IEEE 45*, 10 (October 2007), 47–53. 42, 65, 83, 165, 189

[21] MARINOS, L., AND ENISA. ENISA Threat Taxonomy A tool for structuring threat information INITIAL VERSION 1.0. Tech. rep., JANUARY 2016. 68

[22] PATIDAR, D., AND DUBEY, J. A hybrid approach for dynamic intrusion detection, enhancement of performance and security in manet. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies* (New York, NY, USA, 2016), ICTCS '16, ACM, pp. 81:1–81:5. Available from: `http://doi.acm.org/10.1145/2905055.2905291`. 64

[23] PRIYA, S. B., AND THEEBENDRA, C. A Study on Security Challenges in Mobile Ad Hoc Networks. 64

[24] RAI, B., AND JAIN, P. A. Survey of attacks and security schemes in manet. *Universal Journal of Computers & Technology (UJCT) 1*, 1 (2016). 64

[25] RUSSELL, D., LOOKER, N., LIU, L., AND XU, J. Service-oriented integration of systems for military capability. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)* (2008), IEEE, pp. 33–41. 65

[26] RUSSELL, D., AND XU, J. Service oriented architectures in the delivery of capability. *Proc. of Systems Engineering for Future Capability* (2007). 65

[27] RUSSELL, D., AND XU, J. Service oriented architectures in the provision of military capability. In *UK e-Science All Hands Meeting* (2007), Citeseer. 65

[28] SURI, N. Dynamic Service-oriented Architectures for Tactical Edge Networks. In *Proceedings of the 4th Workshop on Emerging Web Services Technology* (New York, NY, USA, 2009), WEWST '09, ACM, pp. 3–10. Available from: `http://doi.acm.org/10.1145/1645406.1645408`. 42, 65, 83, 165

[29] VASILEIOS, G., WOLTHUSEN, S. D., FLIZIKOWSKI, A., STACHOWICZ, A., NOGALSKI, D., GLEBA, K., AND SLIWA, J. Interoperability of security and quality of service policies over tactical soa. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)* (Dec 2016), pp. 1–7. 63, 103, 146, 214, 227

[30] WANG, H., WANG, Y., AND HAN, J. A security architecture for tactical mobile ad hoc networks. In *Knowledge Discovery and Data Mining, 2009. WKDD 2009. Second International Workshop on* (Jan 2009), pp. 312–315. 65

Chapter 4

Article 1c: Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks

Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks

Norsk informasjonssikkerhetskonferanse - Norwegian Information Security Conference (NISK), Ålesund, 2015, pp. 109-120.

Gkioulos, Vasileios Wolthusen, Stephen D.

Abstract

Tactical networks are typically a combination of wireless ad-hoc and mesh networks, with varying connectivity that may also suffer from temporary partitioning. The implemented mechanisms must provide secure and reliable communication and service delivery, across a wide range of possible network capabilities, structures and composing entities. Furthermore, the ability to compose services dynamically is highly desirable, as is the possibility of accessing services in temporarily available networks.

The adoption of the Service Oriented Architecture paradigm has been recognized as a valuable solution towards the realization of the arising requirements. SOA allows the loose and dynamic coupling of services, implicitly also offering a degree of resilience where services can be substituted if a provider becomes unavailable. In this article we therefore explore the requirements and constraints of the implementation of the SOA paradigm over tactical networks. Aiming to dynamic security policies where policy decision and enforcement points can coincide and be distributed, also incorporating situational knowledge. To allow both (partial) pre-computation and dynamic evaluation of policies. Additionally, we describe a constrained ontology framework for the realization of dynamic security policies over this environment, based on the identified constraints.

4.1 Introduction

The currently deployed tactical systems are based on contemporary C2 and C4I structures of continuously increasing heterogeneity and complexity. Yet, the ongoing introduction of NCW and NEC, significantly increased the requirement for consistent information exchanges, operational flexibility and dynamic adaptation. SOA based mechanisms emerged as a suitable mediator, towards the achievement of these arising requirements. Thus, various studies have evaluated the SOA paradigm, over networks with similar characteristics to the tactical. Additionally, description logic and ontological structures have been recognised to provide the required descriptive power and syntax, in order to capture the semantics of complex environments, into highly enriched security policies. Yet, such mechanisms have not been utilised within the deployed tactical networks and adapted over their distinct characteristics.

The realisation of concrete security mechanisms dedicated to tactical SOA, has to be based on the identification of the relevant constraints, imposed by the nature of this environment. The findings of this procedure can concurrently be used for the definition of the corresponding high level security functional requirements, which can lead to the identification of the appropriate composing elements, structural formulations and operational interactions. In this study, following the aforementioned procedure, we present our findings regarding the constraints of tactical SOA, translate them into the required functional characteristics and propose a suitable baseline framework for the realisation of security infrastructures dedicated to tactical SOA.

4.2 Related work

The tactical environment is continuously and rapidly evolving. Thus, it has been under extensive and diachronic study, both in terms of fundamental warfare analysis [13] and technical evaluation [1, 9, 31, 5]. Such studies provide crucial information, useful for the understanding and incorporation of the distinct governing conditions, into newly designed tactical systems. The nature of the modern tactical environment, promoted the evaluation of the SOA paradigm as a suitable mediator towards the new imposed requirements. Various studies included the evaluation of SOA implementations with the use of web services [22], the evaluation of SOA implementations over disadvantaged networks [17] or tactical EDGE networks [36] including the studies of the IST-090[15]/ IST-118[16] working groups, the evaluation of existing and rising security solutions over tactical SOA [23], as well as other perspectives, such as battle command [24].

Regarding the security perspective, multiple approaches have been defined, for the specification of security policies, in other fields [7, 32, 35].

Yet, the most commonly used mechanisms, such as WS-Security, Ponder [8], SAML [28] or XACML [30], lack the ability of decentralized operation, while they suffer significant expressiveness constraints, when implemented over open and dynamic environments, rendering them inadequate for the tactical ecosystem. Such constraints promoted attempts to combine these mechanisms with ontological representations and logic based systems, integrating this way part of their extensive expressive power [10, 3, 12].

Shortly after, multiple successful efforts managed to fully utilise the expressive power of description logic, for the complete definition of security policies and access control systems [4, 34, 27]. Finin et al. [11] presented a mechanism for the realization of RBAC (Role Based Access Control) with OWL-DL, while Kolovski et al. [19] provided a mapping mechanism of WS-Policies to OWL-DL. Trivellato et al. [37] provided a framework for semantic vocabulary alignment between different ontologies in coalition environments. In the same study it is presented that both, previously established trust management (such as RT [21], Cassandra [2], Peer-Trust [26], Tulip [6]) and semantic frameworks (such as ROWLBAC [11], REI [18], KAOS [38], Kolter et al [20]), lack either in terms of decentralised operation, expressive capturing of semantic values or ease of development and deployment.

The successful undertaken research efforts throughout these fields, promoted the practical application of the SOA paradigm over the strategic domain, with sufficiently dynamic security mechanisms. Yet, the characteristics and constraints imposed by the tactical domain, differ in great extent from those of the strategic. The defined NATO C3 System Architecture Framework [25] does not incorporate a wide variety of such constraints, such as mobility, disruption tolerance and operation over highly congested or otherwise restricted networks, even for currently available services. The German national project RuDi aiming to the definition of a reference service environment, reaches towards applications and security services within the tactical domain. Yet, critical constraints such as the limited storage capacity or computational power of the mobile tactical nodes are not taken under consideration. Furthermore, the international project CoNSIS, focuses on improving and adapting existing enterprise service bus infrastructures into highly mobile networks, without utilizing the known benefits of ontological constructs for security mechanisms.

4.3 The tactical environment

The tactical environment is eminently dynamic, versatile and diverse, depending immensely on the nature of each particular tactical operation.

1. The multitude of the deployed assets may vary from a team of two dismounted soldiers, up to a few thousand elements.

2. The tactical network is required to serve over a highly heterogeneous ecosystem, due to the diverse nature, capabilities and requirements of the deployed platforms. This diversity is presented in various terms, that include mobility, computational power, storage capacity, autonomy, communication capabilities and physical security.

3. Another aspect is the operational and functional diversity of the deployed elements. The various nodes within an AoO are organised in discrete yet interoperable operational groups, with distinct characteristics, operational requirements and goals. Similarly, the elements that constitute these groups, have distinct functional roles and capabilities through a tactical operation.

4. A plethora of information are available within the tactical network, generated by the involved elements, including users, services and equipment. Yet, these blocks of information are of broad dissimilarity in terms that include their nature (alerts, orders, tactical information), type (data, voice, chat, signalling), format, generation frequency or their required quality, reliability and security features.

5. The structure of the tactical environment is highly dynamic, with rapidly changing topology, since new nodes may ender or exit the network at will, while the existing actors move freely within the AoO. Thus, no safe assumptions can be made regarding the existence of continuous connectivity, while extensive delays, communication failures, random network splits/ merges and uncertain service delivery must be expected.

6. The dynamic nature of the tactical environment is further aggravated since some of the deployed actors may be required to operate in coalition environments with discrete security mechanisms, radio silence, low detection, anti jam or low interception status.

7. The presence of adversaries must be considered certain. Their competence should be expected to extend throughout a wide variety of active and passive attacks, including communication disruption, targeted physical attacks and information extraction attempts.

These characteristics clarify the unique nature of the tactical environment, even towards the closely related systems focusing on the strategic domain, while they delineate the additional challenges of coping with the involved dynamics.

4.4 The security perspective of tactical SOA

The combination of the aforementioned constraints can be used to clarify and construct the required functional characteristics of the implemented security mechanisms. These functional characteristics form a parallel iteration of requirements in addition to a set of security goals based on a refined and properly adapted version of the Parkerian Hexad (Confidentiality, Control, Integrity, Authenticity, Availability, and Utility), which can be common for the tactical and the strategic domains. These additional elements require appropriately formulated security mechanisms, since distributed SOA was not designed for such a dynamic environment.

1. The realised security mechanisms have to be highly scalable, incorporating at the same time the various SOA platform service layers alongside with the Quality of Service, communication and infrastructure levels. Thus, requiring an adaptable multilayer implementation.

2. The definition, update, evaluation, enforcement and transmission of security policies must be based on a scalable and dynamic combination of the available resources and cross layer information. This can ensure service delivery, based on dynamic adaptation of the available security mechanisms.

3. The security enforcement procedures must incorporate real time evaluation of the existing tactical conditions, allowing the most suitable utilization of the security policy, taking under consideration the heterogeneity of the involved elements.

4. Due to operational and functional diversity of the deployed elements, the implemented security mechanisms must support the dynamic distribution of both the security policy and the governing conditions. This allows the extension of the overall system scalability, minimises the potential risk due to a compromised node and by promoting node interoperability, allows the complete utilization of the specific capabilities of each tactical node. Furthermore, the security policy distribution can be used in order to promote the identification of occurring collisions, that may require reconciliation.

5. Additionally, due to the constant alterations in terms of connectivity, available bandwidth and network topology, no centralized security dedicated entity can be assumed to operate over the tactical network, since these characteristics raise various constraints, affecting the number of possible invocations or the transmission of complex policy expressions. Thus, the implemented security mechanisms and services must be distributed across all the deployed network elements.

6. Protection mechanisms must be realised regarding both service access and the various objects attached to the services. These mechanisms must incorporate simplified policy expressions or pre-calculated policy decisions, maintaining the capability to evolve into dynamic and on-line evaluated multi-level security constructs, when information and resources are available. This can permit the standalone operation of nodes in a highly disrupted environment and reassures the operation of disadvantaged nodes due to limited resources.

4.5 Dynamic security policies over tactical SOA

As presented at section 4.2, the use of description logic for the formalization of security policies, has been widely proposed and successfully implemented in various domains. Yet, it has not been appropriately adopted and utilised for the specifics of tactical networks. In this article we propose the use of OWL-DL and its fragments to define a baseline security policy framework, appropriately adapted to the aforementioned specifics of the tactical environment. The decision of selecting OWL-DL is based (as presented at section 4.2) on the known vulnerabilities of other mechanisms into capturing the required semantics, operating over highly dynamic and distributed environments or ease of development and deployment.

4.5.1 Structuring security policies for tactical SOA

In a tactical SOA the services are orchestrated in order to support every mission aspect, while the deployed nodes are both service providers and consumers. The proposed framework is presented at figure 4.1. This allows the unambiguous definition of the various tactical domains (including but not limited to planning, protection, diligence, response and detection), capabilities (including but not limited to core, application, communication and inter-domain), the various actions towards these capabilities and the governing rules of these actions. The proposed structure minimises tree impurities within the security core ontology, something that reduces the overall complexity, inherently affecting the complexity of policy distribution and reconciliation procedures.

The construction of the required security policy incorporates a distributed database for the definition of the governing rules, including the wide plethora of static or dynamic multi-domain information available within the tactical network, based on the requirements of each operation. Such information can refer to various attributes regarding the nature and requirements of the involved actors, the real time and past operational conditions of the network (including resource availability) and the occurring element actions and interactions. These information, in order to maintain the purity of the

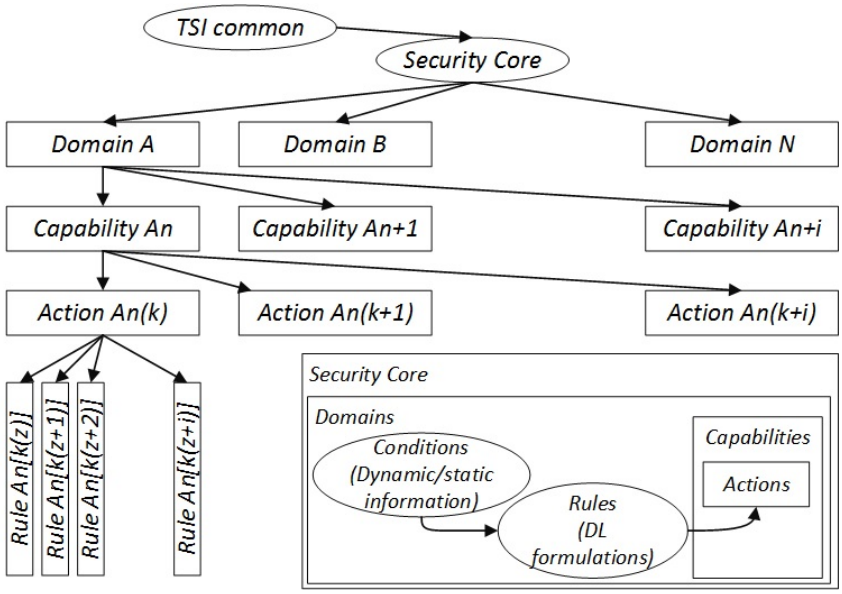

Figure 4.1: Security policy structure.

security ontology, must be layered as referring to 1 - Services, 2 - Information, 3 - Network status, 4 - Radio status, 5 - Node status, 6 - Subjects.

The proposed structure allows for a dual notion of dynamism, regarding the operation of the overall security policy. The first dynamic characteristic occurs by the definition of the rules corresponding to each action. Each rule-set spans from simple pre-calculated expressions, that allow the operation of nodes with limited resources, towards expressions of increased complexity, that incorporate a variable set of static and dynamic information, in order to maintain support of security services as the tactical mission evolves. The second dynamic characteristic occurs by the definition and complex relationships of the dedicated Domain, Capability and Action substructures. These elements exploiting the expressive power of description logic, proceed to on-line evaluation of the current network status, based on the defined information, after every service invocation. Thus, achieving the selection of the appropriate governing rule or suggesting a suitable service substitution.

4.5.2 Conceptualization of tactical policy framework

The ontological conceptualization of the described framework, over the hierarchical structure of a tactical network, can be achieved by the use of unary

and binary predicates. Unary predicates within the defined context represent data, services, users, terminals and conditions, while binary predicates represent the possible relationships among them. Thus, a broad definition of a network can be achieved by defining the distinct elements and their relations, structuring an interpretation of the current and past status of the overall ecosystem.

The definition of the required tactical terminology is achieved by T-box definitions. The T-Box allows the unique and acyclic concept definition in terms of sufficient and necessary conditions. Thus, each of the defined concepts throughout the required tactical domains, is gradually structured through a complex combination of atomic concepts that declare these conditions. A-Box role, on the contrary, is oriented to instance identification, specifying whether a specific individual is an instance of the concepts defined within the T-Box. This is primarily achieved by concept and role assertions. It must be noted at this point, that the required concept expressiveness may affect the overall computational and reasoning complexity. Additionally, the assertional knowledge is defined at the A-Box at the initiation of the operation for the static elements, while the dynamic elements evolve as the tactical operation progresses. This flexibility is exploited by the proposed model, in order to make best use of the dynamic semantic information for policy decisions. Thus a knowledge base is defined as a structured pair of a T-Box and an A-box (T/ A). This procedure is presented at figure 4.2. When the complete tactical terminology has been constructed, assertional knowledge such as Has_Current_Status, Can_Be_Substituted and Has_Provider, can be constructed and altered on-line, in order to define or identify a specific service as an instance.

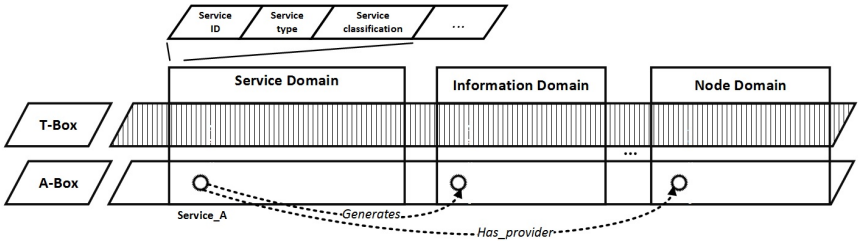

Figure 4.2: Security policy conceptualization.

4.5.3 Formal representation of security policies and situational knowledge

The formal representation of the described security policy framework, requires a description logic fragment, with sufficient expressive power to ac-

commodate the definition of the various static and dynamic elements and their complex relations. The selected DL-fragment, has been identified that in order to achieve the adequate and precise capturing of the involved semantics must be based on ALC, but also include the additional elements of role hierarchy, nominals, inversion, cardinality, functionality properties, qualified cardinality restrictions and role inclusion. A suitable DL-fragment is SHOIN(D) that includes all the aforementioned elements in addition to supplementary data related properties and values. Furthermore, SHOIN(D) represents a fragment of OWL DL [33], it is supported by widely used ontology editors, such as Protege, while a plethora of efficient reasoners exist. The core of SHOIN(D) relies on the common syntax outlined by one of the basic description logic fragments called ALC (Attribute Language with Complements). And provides the following constructors:

	(Name) Description	Syntax
1	(Top) Universal concept	$\top$
2	(Bottom) Empty concept	$\bot$
3	Atomic concept	A
4	Concept union	$\sqcup$
5	Concept intersection	$\sqcap$
6	Concept negation	$\neg$
7	Universal value restriction	$\forall$
8	Limited existential restriction	$\exists$
9	(Cardinality) Unqualified value restrictions	$\leq$,$\geq$,= (n R)
10	(Cardinality) Qualified value restrictions	$\leq$,$\geq$,= (n R.C)
11	Nominals	$\{i_1 \dots i_n\}$
12	Atomic role hierarchy and inverse roles	R, R^{-1}
13	Sub-role	$\subseteq$
14	Universal role assertion	$\cup$
15	Sub-class	$\sqsubseteq$
16	Equivalence	$\equiv$
17	Inversion	$^-$

Table 4.1: Subset constructors available in the SHOIN(D) DL fragment.

The full list of the semantics supported by OWL-DL and the suggested description logic fragment can be seen at [29]. As presented earlier the terminology of the tactical network is defined within the T-Box and may contain simplified or complex expressions such as:

Equation 4.1:
$Service \equiv individual \sqcap \exists has\_Service\_ID.\ \bot$

Equation 4.2:
$Service\_Type1 \equiv Service \sqcap \exists Has\_Functionality.Messaging \sqcap \exists Has\_Status.Online$

Equation 4.3:
$Available\_Service \equiv Service(\leq 1 Has\_Local\_Provider \sqcup (\geq 2 Has\_Local\_Provider \sqcap \exists Has\_Local\_Provider.Active))$

Instance identification within the A-Box can be achieved primarily by concept and role assertions, using the presented constructors as:

Equation 4.4:
$File \sqcap Text(msg1) : msg1\ is\ a\ text\ file$ (concept assertion)

Equation 4.5:
$hasSource(msg1, Service1) : Service1\ is\ the\ source\ of\ msg1$ (role assertion)

Thus, defining services, information, nodes and subjects as individuals, can be achieved using simple world definitions, over static and dynamic information, over the universal A-box as:

Equation 4.6:
$Has\_Given\_Name(UserA, Nikolaos)$
$Has\_ID(UserA, 522091)$
$Has\_Rank(UserA, Captain)$
$Has\_Current\_Location(UserA, AoO1)$
$Has\_Operational\_Group(UserA, OG2)$

Moreover, the relationships among the network entities can be defined using membership assertions, such as those presented in equations 4.4 and 4.5. Similarly, the current user of a node, the resource availability of a terminal, the operational state of a service and the rest of the available information regarding the defined domains can be represented.

The construction of the required policy expression branches, based on the described framework, can be organized in discrete requirement sets that correspond to distinct security levels as:

Node_Can_Be_Accessed(Node1;Node_Requirements_Set-1)
...
Node_Can_Be_Accessed(Node1;Node_Requirements_Set-n)

Other policy domains, referring for example to service substitution, can also be defined similarly as:

Service_Can_Be_Substituted(Service_Type_1;Service_Substitution_Set-1)

...
Service_Can_Be_Substituted(Service_Type_1;Service_Substitution_Set-n)

Additionally to Terminology/ Assertion pairs (T/ A) that can be defined using the available constructors, rules can also be used for knowledge representation. The use of rules significantly increases the expressive power, allowing the definition of additional security constraints such as separation of duty. A triplet in the form of (T/ A/ R) can be used for the definition of more complex relations within the tactical environment. A rule can be defined having the form:

Equation 4.7:
$KPrivate \sqsubseteq \forall Uses.NodeTypeA$

Stating that all the individuals who are defined within the A-Box to have rank equivalent to private, make use of a specific type of node, defined as NodeTypeA within the T-Box. Such rules can be defined utilizing SWRL (Semantic Web Rule Language) [14], which is based on a *"combination of the OWL DL and OWL Lite sublanguages of the OWL Web Ontology Language with the Unary/Binary Datalog RuleML sublanguages of the Rule Markup Language"*.

4.6 Scenario

To illustrate the identified dynamics of the tactical environment and the corresponding functionalities of the defined framework let us assume the following scenario.

- Entity A requires service B.
- Entity A requires service B to satisfy a set of properties X and service provider to satisfy a set of properties K.
- Service B is provided by nodes C and D.
- Node C offers properties set X, while node D offers properties sets X and Y.
- The property sets are evaluated and node C is selected as the service provider.
- Entity A is evaluated by node C, since node C and service B require every invoking entity to satisfy a minimum set of requirements Z.
- Node C identifies that will become unavailable. Entity A is informed and service delivery is delegated to node D.

Entity A may be a user or another service defined based on the network terminology, as presented in figure 4.2, based on concept and role assertions, similar to those of equations 4.4 and 4.5. Similarly, service B and nodes C, D are equally defined following the same procedure. Thus, entity A queries the local knowledge base, in order to identify a service and a service provider that complies with the corresponding requirement sets X and K. The requirement sets and the queries towards the knowledge base, are a set of the defined policy rules, appropriately selected by the corresponding Domain, Capability and Action substructures, as presented in figure 4.1.

The structure of these substructures, is of high significance at this point, since the deduction capacity of the node and the available resources, at the time of the query initiation, are used to define the maximum complexity of the policy expression used to identify the service/ service provider. Thus, the policy expression might be a precomputed value, a simplified expression, or expressions of increased complexity, incorporating multiple combinations of static and dynamic information.

Assuming that both nodes C and D, return from the query as providers of the service related requirements set X, the service provider can be selected based on the node/ network/ radio related requirements set K. Thus, in this simplified scenario, node C is selected as the service provider, based among others due to current resource availability and because it belongs to the same operational group with entity A (Providing this way a higher probability of maintaining closer proximity for longer period).

Similarly, upon receipt of the service invocation, node C makes use of the corresponding policy branch in order to evaluate the defined set of parameters regarding the various domains. Thus, entity A is evaluated as a legitimate user, while network, node, radio and other parameters are also evaluated in order to identify the feasibility of the request and the most suitable serving approach.

After negotiation of the interaction parameters among the entity A and node C, based on the specified security policy branches, the service delivery is initiated. An additional advantage of the described framework, resulting from the on-line evaluation of various dynamic and static information, is the evaluation of the interaction itself, making possible to identify and anticipate possible parameter alterations. Thus, service delivery can be delegated by node C to node B, based on the previously established interaction agreement among entity A and node D.

4.7 Conclusions

Through this article, the findings of our study regarding the constraints imposed by the nature of tactical SOA implementations have been presented. These constraints have been translated into the corresponding functional re-

quirements for the implementation of security mechanisms dedicated to tactical networks. Furthermore, a security policy framework of suitable structural characteristics has been suggested, making use of the expressive power of description logic and ontological constructs, for the sufficient realisation of these requirements.

Our future plans include the further evaluation and refinement of the proposed framework. More precisely the study of how the structure of the higher level ontological constructs can affect the efficiency and efficacy of the overall mechanism. Early results suggest that the structure of the ontological constructs is critical, in order to fully exploit the expressive power provided by description logic, minimize resource utilization and achieve compact security policy definition and reasoning. Additionally, we intent to identify suitable mechanisms for the apriory distribution, on-line update and reconciliation of the security policy, aiming to maximize the node cooperation, while minimizing and allocating the computational cost of each policy decision.

Acknowledgments

The results described in this work were obtained as part of the EDA IAP4 project TACTICS (Tactical Service Oriented Architecture). The TACTICS project is jointly undertaken by Patria (FI), Thales Communications & Security (FR), Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE (DE), Thales Deutschland (DE), Selex ES (IT), Thales Italia (IT), Gjøvik University College (NO), ITTI (PL), Military Communication Institute (PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980.

Bibliography

[1] BAR-NOY, A., CIRINCIONE, G., GOVINDAN, R., KRISHNAMURTHY, S., LAPORTA, T. F., MOHAPATRA, P., NEELY, M., AND YENER, A. Quality-of-information aware networking for tactical military networks. In *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (March 2011), pp. 2–7. 13, 83, 165

[2] BECKER, M., AND SEWELL, P. Cassandra: distributed access control policies with tunable expressiveness. In *Policies for Distributed Systems and Networks, 2004. POLICY 2004. Proceedings. Fifth IEEE International Workshop on* (June 2004), pp. 159–168. 84, 143, 165

[3] BEN BRAHIM, M., CHAARI, T., BEN JEMAA, M., AND JMAIEL, M. Semantic Matching of WS-Security Policy Assertions. In *Service-Oriented Computing - ICSOC 2011 Workshops*, vol. 7221 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2012, pp. 114–130. Available from: http://dx.doi.org/10.1007/978-3-642-31875-7_13. 42, 84, 165

[4] BLANCO, C., LASHERAS, J., VALENCIA-GARCIA, R., FERNANDEZ-MEDINA, E., TOVAL, A., AND PIATTINI, M. A systematic review and comparison of security ontologies. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on* (March 2008), pp. 813–820. 84, 165, 189

[5] BURBANK, J. L., CHIMENTO, P. F., HABERMAN, B. K., AND KASCH, W. T. Key challenges of military tactical networking and the elusive promise of manet technology. *IEEE Communications Magazine 44*, 11 (November 2006), 39–45. 13, 64, 83, 165

[6] CZENKO, M., DOUMEN, J., AND ETALLE, S. Trust management in p2p systems using standard tulip. In *Trust Management II*, Y. Karabulut, J. Mitchell, P. Herrmann, and C. Jensen, Eds., vol. 263 of *IFIP The International Federation for Information Processing*. Springer US, 2008, pp. 1–16. Available from: http://dx.doi.org/10.1007/978-0-387-09428-1_1. 84, 143, 165

[7] DAMIANOU, N., BANDARA, A., SLOMAN, M., AND LUPU, E. A survey of policy specification approaches. *Department of Computing, Imperial College of Science Technology and Medicine, London 3* (2002), 142–156. 18, 42, 83

[8] DAMIANOU, N., DULAY, N., LUPU, E., AND SLOMAN, M. The Ponder policy specification language. *Policy 1* (2001), 18–38. 18, 19, 84, 143, 165, 215

[9] ELMASRY, G. F. A comparative review of commercial vs. tactical wireless networks. *IEEE Communications Magazine 48*, 10 (October 2010), 54–59. 12, 42, 83, 165

[10] FERRINI, R., AND BERTINO, E. Supporting RBAC with XACML + OWL. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT '09)* (Stresa, Italy, June 2009), B. Carminati and J. Joshi, Eds., ACM Press, pp. 145–154. 84, 165, 214

[11] FININ, T., JOSHI, A., KAGAL, L., NIU, J., SANDHU, R., WINSBOROUGH, W. H., AND THURAISINGHAM, B. ROWLBAC - Representing Role Based Access Control in OWL. In *Proceedings of the 13th Symposium on Access control Models and Technologies* (Estes Park, Colorado, USA, June 2008), ACM Press. 84, 143, 165, 189

[12] HELIL, N., AND RAHMAN, K. Extending XACML profile for RBAC with semantic concepts. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on* (Oct 2010), vol. 10, pp. V10–69–V10–74. 84, 165, 214

[13] HORNE, G., AND LEONARDI, M. *Maneuver Warfare Science 2001*. Marine Corps Combat Development Command, 2001. 42, 83, 165

[14] HORROCKS, I., PATEL-SCHNEIDER, P., BOLEY, H., TABET, S., GROSOF, B., AND DEAN, M. SWRL: A Semantic Web Rule Language - Combining OWL and RuleML. Tech. rep., W3C-World Wide Web Consortium, 2004. 92

[15] IST-090 TASK GROUP. Service oriented architecture (SOA) challenges for real time and disadvantaged grid (IST-090). `https://www.cso.nato.int/Activity_Meta.asp?ACT=1830`, April 2014. 42, 83, 165

[16] IST-118 TASK GROUP. SOA recommendations for disadvantaged grids in the tactical domain (IST-118). `https://www.cso.nato.int/ACTIVITY_META.asp?ACT=2293`. 42, 83, 165

[17] JOHNSEN, F., BLOEBAUM, T., SCHENKELS, L., FISKE, R., VAN SELM, M., DE SORTIS, V., VAN DER ZANDEN, A., SLIWA, J., AND CABAN,

P. SOA over disadvantaged grids experiment and demonstrator. In *Communications and Information Systems Conference (MCC), 2012 Military* (Oct 2012), pp. 1–8. 42, 83, 165, 214

[18] KAGAL, L., FININ, T., PAOLUCCI, M., SRINIVASAN, N., SYCARA, K., AND DENKER, G. Authorization and privacy for semantic web services. *Intelligent Systems, IEEE 19*, 4 (Jul 2004), 50–56. 84, 143, 165

[19] KOLOVSKI, V., PARSIA, B., KATZ, Y., AND HENDLER, J. Representing web service policies in OWL-DL. In *In International Semantic Web Conference (ISWC* (2005), pp. 6–10. 84, 165, 189

[20] KOLTER, J., SCHILLINGER, R., AND PERNUL, G. Building a distributed semantic-aware security architecture. In *New Approaches for Security, Privacy and Trust in Complex Environments*, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, Eds., vol. 232 of *IFIP International Federation for Information Processing*. Springer US, 2007, pp. 397–408. Available from: http://dx.doi.org/10.1007/978-0-387-72367-9_34. 84, 143, 165

[21] LI, N., MITCHELL, J., AND WINSBOROUGH, W. Design of a role-based trust-management framework. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on* (2002), pp. 114–130. 84, 143, 165

[22] LUND, K., EGGEN, A., HADZIC, D., HAFSOE, T., AND JOHNSEN, F. Using web services to realize service oriented architecture in military communication networks. *Communications Magazine, IEEE 45*, 10 (October 2007), 47–53. 42, 65, 83, 165, 189

[23] MAULE, R. W., AND LEWIS, W. C. Security for distributed soa at the tactical edge. In *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE* (Oct 2010), pp. 13–18. 15, 83, 165

[24] MAYOTT, G., SELF, M., MILLER, G. J., AND MCDONNELL, J. S. Soa approach to battle command: simulation interoperability, 2010. Available from: http://dx.doi.org/10.1117/12.851912. 83, 165

[25] NATO. Nato c3 classification taxonomy. https://www.act.nato.int/article-8a, 2012 March. 84, 149

[26] NEJDL, W., OLMEDILLA, D., AND WINSLETT, M. Peertrust: Automated trust negotiation for peers on the semantic web. In *Secure Data Management*, W. Jonker and M. Petkovi, Eds., vol. 3178 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2004, pp. 118–132. Available from: http://dx.doi.org/10.1007/978-3-540-30073-1_9. 84, 143, 165

[27] NGUYEN, V. Ontologies and information systems: A literature survey, 6 2011. Available from: http://hdl.handle.net/1947/10144. 84, 165, 189

[28] OASIS. OASIS Security Services (SAML) TC. Available from: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security. 84, 143, 165, 214

[29] PATEL-SCHNEIDER, P. F., HAYES, P., AND HORROCKS, I. OWL Web Ontology Language Semantics and Abstract Syntax - OWL Working Group, February 2004. Available from: http://www.w3.org/TR/owl-semantics/. 90, 169

[30] RAMLI, C. D. P. K., NIELSON, H. R., AND NIELSON, F. The Logic of XACML. *Science of Computer Programming 83* (Apr. 2014), 80–105. 84, 143, 165, 214

[31] SHI, V. Evaluating the performability of tactical communications networks. *Vehicular Technology, IEEE Transactions on 53*, 1 (Jan 2004), 253–260. 42, 83, 165

[32] SLOMAN, M., AND LUPU, E. Security and management policy specification. *IEEE Network 16*, 2 (Mar 2002), 10–19. 18, 42, 83

[33] SMITH, M. K., WELTY, C., AND MCGUINNESS, D. L. OWL Web Ontology Language Guide-OWL Working Group, November 2009. Available from: http://www.w3.org/TR/2004/REC-owl-guide-20040210/#OwlVarieties. 90

[34] SOUAG, A., SALINESI, C., AND COMYN-WATTIAU, I. Ontologies for security requirements: A literature survey and classification. In *Advanced Information Systems Engineering Workshops*, M. Bajec and J. Eder, Eds., vol. 112 of *Lecture Notes in Business Information Processing*. Springer Berlin Heidelberg, 2012, pp. 61–69. Available from: http://dx.doi.org/10.1007/978-3-642-31069-0_5. 84, 165, 189

[35] STONE, G., LUNDY, B., AND XIE, G. Network policy languages: a survey and a new approach. *Network, IEEE 15*, 1 (Jan 2001), 10–21. 42, 83

[36] SURI, N. Dynamic Service-oriented Architectures for Tactical Edge Networks. In *Proceedings of the 4th Workshop on Emerging Web Services Technology* (New York, NY, USA, 2009), WEWST '09, ACM, pp. 3–10. Available from: http://doi.acm.org/10.1145/1645406.1645408. 42, 65, 83, 165

[37] TRIVELLATO, D., ZANNONE, N., GLAUNDRUP, M., SKOWRONEK, J., AND ETALLE, S. A semantic security framework for systems of systems. *International journal of cooperative information systems 22*, 01 (2013), 1350004. 20, 84, 143, 165, 189, 190, 215

[38] USZOK, A., BRADSHAW, J., JEFFERS, R., SURI, N., HAYES, P., BREEDY, M., BUNCH, L., JOHNSON, M., KULKARNI, S., AND LOTT, J. Kaos policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement. In *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks* (June 2003), pp. 93–96. 18, 19, 84

Chapter 5

Article 2a: Security Infrastructure for Service Oriented Architectures at the Tactical Edge

Security Infrastructure for Service Oriented Architectures at the Tactical Edge

11th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), Torino, 2017, Springer, AISC, volume 611, pp. 310-322

Gkioulos, Vasileios Wolthusen, Stephen D.

Abstract

The requirement for enabling NCW through the accommodation of network-enabled capabilities, promoted the use of SOA within military networks. The initial response of the academic and industrial communities was to utilize standard enterprise SOA. The developed solutions were well adjusted to the strategic domain, where node and network constraints were minimal. Yet, experience gained from the battlefields of the last decade, has proven that the tactical domain imposes a set of unique constraints, that render such solutions inefficient for the tactical edge.

The project TACTICS, supported by EDA, focuses on the study and development of a SOA dedicated to tactical networks. In this paper we present the designed security service architecture, as developed in accordance to the requirements identified in our earlier studies. Each service is presented as an architectural element within the TACTICS TSI, aiming to highlight the distinct functionalities of the security infrastructure towards the efficient enforcement of security controls at the tactical edge.

5.1 Introduction

The introduction of SOA across the strategic domain of military networks has been promoted by the increasing requirement for the integration of NEC, within the developed C2 and C4I systems. Extending this paradigm to the tactical domain is expected to allow the widespread incorporation of

NCW, by improving situational awareness and increasing network flexibility, adaptability and responsiveness at the tactical edge.

However, standard enterprise SOA have been proven across the AoO of recent conflicts to be unsuitable for tactical networks, due to their rapidly evolving nature and constrained resources. The project TACTICS [1] is oriented towards the theoretical and experimental analysis of contemporary tactical networks, in respect to the feasibility and required adaptations for the deployment of SOA. Consequently, and in accordance to these studies, a TSI has been defined and experimentally demonstrated. The TSI architecture [2] was developed according to the NATO Architecture Framework 3.1, including twenty discrete architectural perspectives.

Focusing on the security aspects of such an architecture, our study was initiated by analysing system specific constraints and requirements, arising due to terminal and network characteristics across the three mission stages (preparation, execution, debrief). This allowed the identification of fine-grained security requirements and protection goals, maintaining the necessary distinction between the communication [5] and service domains [8].

Accordingly, these requirements have been translated into corresponding functional characteristics, for a security policy framework and service infrastructure, that would be suitable for the investigated environment. Furthermore, an extended state-of-the-art review, revealed the weaknesses of existing mechanisms but also suitable adaptations that would satisfy the identified requirements under the imposed constraints [3]. These initial studies, allowed us to analyse, define and develop a suitable security policy framework [6], along with the corresponding distribution [7], reconciliation [4] and QoS interoperability [9] mechanisms.

In this article we present the core security service infrastructure, as developed within the TACTICS TSI in accordance to the aforementioned studies. These components are suitably adjusted towards satisfying the identified requirements, by facilitating the operation of the developed security policy framework and supporting mechanisms. The remainder of this paper is structured as follows: Section 5.2 presents the functionalities and interactions of each developed service, as an architectural element towards the extraction of valid policy decisions. Subsequently, section 5.3 includes a discussion over the operational complexity of the security service infrastructure, in accordance to early results from the ongoing field and laboratory experiments/ demonstrations.

5.2 TACTICS Security Architecture

The developed security architecture, consists of two distinct groups of services, namely core and functional. The functional services are responsible for the enforcement of the requisite protection goals, by instantiating the

distinct mechanisms (e.g. encryption algorithms, access control, intrusion detection), while the core security services are responsible for the governance of these mechanisms, in accordance to predefined security policies. In this section we present these components (Figure 5.1), aiming to highlight the processes involved in the extraction of suitable policy decisions (Figures 5.2 and 5.3). It must be noted that the security policy framework developed within TACTICS for the accommodation of the requirements imposed by contemporary tactical SOA, has been presented earlier in detail [6] and is outside the scope of this article.

The main functionalities of each service as presented in figures 5.1, 5.2 and 5.3 can be summarised as:

- **Security Handling service**
  1. Initiate the internal policy decision extraction process.
  2. Store and identify the applicability of precomputed policy decisions.
- **Policy Management service**
  1. Control the policy decision extraction process.
  2. Prioritize pending policy decision requests.
- **Policy Decision Point service**
  1. Securely store the prioritized rule stacks that have been defined for each available policy decision request.
- **Metadata Handling service**
  1. Accommodate the defined ontological knowledge base (Including both the Terminological-box and Assertional-box) and the selected inference engines.
  2. Extraction of policy decisions.
- **Contextual Monitoring service**
  1. Monitoring and collection of dynamic attributes.
  2. Generation of statistical and aggregated data.
  3. Triggering of event-driven policy decisions to the Security Handling service.
  4. Update of Metadata Handling service A-box to current values.
- **Policy Enforcement Point service**
  1. Translation and enforcement of extracted policy decisions.

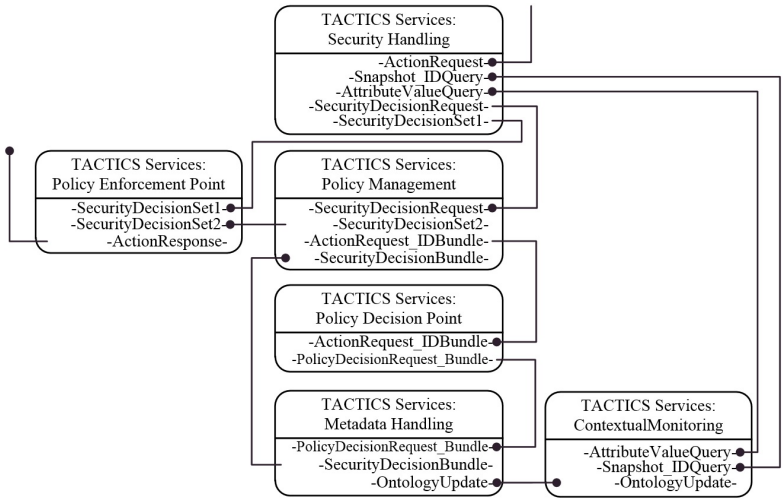

Figure 5.1: Interfaces of the developed core security services.

Figure 5.2: Sequence diagram for valid precomputed policy decisions.

5.2.1 Security Handling Service

Description: The Security Handling (SH) service operates as the internal to the security architecture action (policy decision) requester. The service can be invoked either externally (by a predefined set of core and functional services, for which the required interfaces have been established for the in-

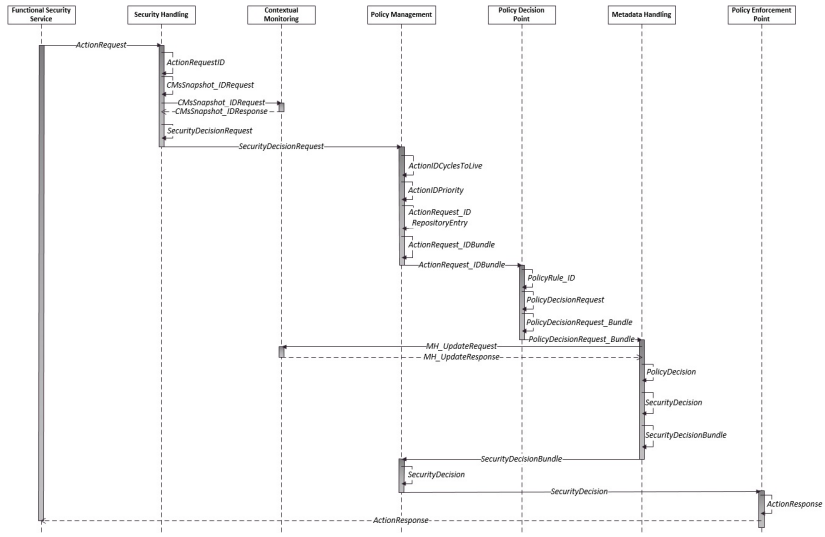

Figure 5.3: Sequence diagram for the on-line extraction of policy decision.

vocation of corresponding policy decisions) or internally (by the Contextually Monitoring (CM) service, for event-driven policy decisions). The service accommodates precomputed policy decisions for the reduction of the computational overhead imposed by the security architecture. These are established at the mission preparation stage, according to a statistical analysis of previous invocation logs and the use of computational intelligence methodologies. Thus, precomputed policy decisions can be established for a constraint range of the required semantics, and after local evaluation, be directly applied without the invocation of the complete security service stack (Figure 5.2). When such precomputed policy decisions are not available or applicable, the SHs must compose and forward a security decision request to the subsequent security services, providing all the required information for the adaptation, prioritization and successful extraction of valid policy decisions.

Invocation: Invocation Originator $\Longrightarrow$ Invocation Form

1. Set of core and functional services (RequestorID) $\Longrightarrow$ ActionRequest.

2. Contextual Monitoring (CM) service $\Longrightarrow$ Pre-established ActionRequest according to attribute threshold alert.

Functionalities: Internal=*, Input=$\rightharpoonup$, Output=$\leftharpoonup$
1-$\rightharpoonup$ Receive ActionRequest
2-$*$ Generate ActionRequest_ID

3-∗ Identify existence of precomputed PolicyDecision. According to ActionRequest_ID
a-∗ IF(TRUE)
i-∗ Identify required attributes
ii-∗ Generate AttributeValuesRequest
iii-⇜ Send AttributeValuesRequest to CMs for timely values
iv-⇝ Receive AttributeValuesResponse from CMs
v-∗ Evaluate attributes of precomputed PolicyDecision
1-∗ IF(TRUE)
a-∗ Generate SecurityDecision
b-⇜ Send SecurityDecision to PEPs for enforcement
2-∗ IF(Not TRUE)
a-∗ Generate CMsSnapshot_IDRequest
b-⇜ Send CMsSnapshot_IDRequest to CMs
c-⇝ Receive CMsSnapshot_IDResponse from CMs
d-∗ Generate SecurityDecisionRequest
e-⇜ Send SecurityDecisionRequest to PMs
b-∗ IF(Not TRUE)
i-∗ Generate CMsSnapshot_IDRequest
ii-⇜ Send CMsSnapshot_IDRequest to CMs
iii-⇝ Receive CMsSnapshot_IDResponse from CMs
iv-∗ Generate SecurityDecisionRequest
v-⇜ Send SecurityDecisionRequest to PMs

5.2.2 Policy Management Service

Description: The Policy Management (PM) service operates as the controller of the security services that are involved in the policy decision extraction process. The PMs can be explicitly invoked by the Security Handling (SH) service, or execute functionality according to the input received from the Metadata Handling (MH) service. The invocation from the SHs includes all the required information for the management of a viable policy decision extraction within a security decision request. In addition to the action request related elements, an aggregated metric of the available local node resources (for the prioritization of policy decision requests) and a refresh alert based on predefined constraints (for the update of the MHs to the current state of dynamic semantics) are also included. Upon receipt of a security decision request, the corresponding cycles to live and priority are identified according to the received available resources metric. Consequently, a corresponding entry is generated and included within a repository with all the pending security decision requests. The repository entries are prioritized and a bundle is created, including those requests that can currently be served. The cycles to live of those requests are reduced and the bundle is

forwarded to the Policy Decision Point (PDP) service. It must be noted that the cycles to live metric is critical, since it affects the maximum complexity of the policy rule that will be used for the resolution of the security decision request.
Invocation: Invocation Originator $\Longrightarrow$ Invocation Form

1. Security Handling (SH) service $\Longrightarrow$ SecurityDecisionRequest.
2. Metadata Handling (MH) service $\Longrightarrow$ SecurityDecisionBundle.

Functionalities: Internal=*, Input=$\rightharpoonup$, Output=$\leftharpoondown$

- For invocation type 1:
  1-$\rightharpoonup$ Receive SecurityDecisionRequest from SHs
  2-$*$ Extract RefreshAlert from SecurityDecisionRequest
  3-$*$ Extract ResourceAvailability from SecurityDecisionRequest
  4-$*$ Identify ActionIDCyclesToLive (For the received ActionID)
  5-$*$ Identify ActionIDPriority (For the received ActionID)
  6-$*$ Generate ActionRequest_IDRepositoryEntry
  7-$*$ Update ActionRequest_IDRepository (Enter new entry)
  8-$*$ Prioritize ActionRequest_IDRepository (According to 3, 4, 5)
  9-$*$ Generate ActionRequest_IDBundle
  10-$*$ Update (Reduce by one) ActionIDCyclesToLive in ActionRequest_IDRepository (For those included in the ActionRequest_IDBundle)
  11-$\leftharpoondown$ Send ActionRequest_IDBundle to PDPs
  12-$*$ Update ActionRequest_IDRepository (Remove entries with ActionIDCyclesToLive equal to zero)

- For invocation type 2:
  1-$\rightharpoonup$ Receive SecurityDecisionRequest from MHs
  2-$*$ Extract PolicyDecision /s
  3-$*$ Extract ActionRequest_ID /s
  a-$*$ IF(PolicyDecision TRUE)
  i-$*$ Generate SecurityDecision /s
  ii-$\leftharpoondown$ Send SecurityDecision/s to PEPs for enforcement
  iii-$*$ Delete ActionRequest_IDRepositoryEntry /s
  b-$*$ IF(PolicyDecision NotTRUE) OR IF(ActionRequest_IDRepository NotEMPTY)
  i-$*$ Prioritize ActionRequest_IDRepository
  ii-$*$ Generate ActionRequest_IDBundle
  iii-$*$ Update (Reduce by one) ActionIDCyclesToLive in ActionRequest_IDRepository (For those included in the ActionRequest_IDBundle)
  iv-$\leftharpoondown$ Send ActionRequest_IDBundle to PDPs
  v-$*$ Update ActionRequest_IDRepository (Remove entries with ActionIDCyclesToLive equal to zero)

5.2.3 Policy Decision Point Service

Description: The Policy Decision Point (PDP) service operates as a repository of the predefined policy rules. Each ActionID is mapped at the mission preparation stage to a set of ActorIDs, SubjectIDs and RequestorIDs in accordance to a corresponding set of semantics (referring to Services, Information, Networks, Radios, Nodes and Subjects). These mappings constitute the predefined policy rules. Thus, a set of prioritized policy rules of increasing granularity are defined for any given range of the allowed ActionRequest_IDs. Furthermore, an escape rule of least priority is defined for each ActionRequest_ID range, in order to allow the enforcement of security policy decisions under heavily constrained local-node and radio resources. The received ActionIDCyclesToLive indicator defines which of the prioritized rules should be utilized for the given policy reasoning cycle. Accordingly, upon receipt of an ActionRequest_IDBundle, the individual ActionRequest_IDs are separated and bound to the corresponding policy rules (PolicyRule_ID). This is achieved by the individual evaluation of their ActionIDCyclesToLive and rule identification across their predefined rulesets. The generated PolicyDecisionRequest_Bundle contains these ActionRequest_ID/ PolicyRule_ID pairs and the received RefreshAlert indicator.
Invocation: Invocation Originator $\Longrightarrow$ Invocation Form

1. Policy Management (PM) service $\Longrightarrow$ SecurityDecisionRequest.

Functionalities: Internal=*, Input=$\rightharpoonup$, Output=$\leftharpoondown$
1-$\rightharpoonup$ Receive ActionRequest_IDBundle from PMs
2-$*$ Extract RefreshAlert from ActionRequest_IDBundle
3-$*$ Extract individual ActionRequest_ID / ActionIDCyclesToLive pairs
4-$*$ Identify PolicyRule_ID according to ActionIDCyclesToLive
5-$*$ Generate PolicyDecisionRequest /s
6-$*$ Generate PolicyDecisionRequest_Bundle
7-$\leftharpoondown$ Send PolicyDecisionRequest_Bundle to MHs

5.2.4 Metadata Handling Service

Description: A variety of semantic web frameworks can be used for the implementation of the Metadata Handling (MH) service, such as CubicWeb, RDF4J (Sesame), Mulgara, Open Semantic Framework and Jena. The MHs receives a bundle of policy decision requests and updates the local ontology, if required so by the received RefreshAlert. The value of the RefreshAlert originates from the Contextual Monitoring (CM) service (From CMsSnapshot_IDResponse), which bound to an ActionRequest initiation, is used to update the local ontology through the MH_UpdateRequest/ Response process. After this update, the exact functionality order depends on the selected

semantic web framework. Yet, the required functionalities are: Structure ontological construct > Invoke reasoner > Query local ontology (According to the received PolicyRule_ID) for policy decision. The result of this process is then matched with the corresponding ActionRequest_ID and transferred back to the Policy Management (PM) service.
Invocation: Invocation Originator $\Longrightarrow$ Invocation Form

1. Policy Decision Point (PDP) service $\Longrightarrow$ PolicyDecisionRequest_Bundle.

Functionalities: Internal=*, Input=$\rightharpoonup$, Output=$\leftharpoondown$
1-$\rightharpoonup$ Receive PolicyDecisionRequest_Bundle from PDPs
2-$*$ Extract RefreshAlert
a-$*$ IF RefreshAlert TRUE
i-$\leftharpoondown$ i. Send MH_UpdateRequest to Contextual Monitoring service
ii-$\rightharpoonup$ Receive MH_UpdateResponse from CMs
iii-$*$ Update local ontology
3-$*$ Extract PolicyDecisionRequest/ s from PolicyDecisionRequest_Bundle
4-$*$ Create reasoner
5-$*$ Insert ontological terminology and assertions
a-$*$ For(all PolicyDecisionRequest/ s)
i-$*$ Extract PolicyRule_ID from PolicyDecisionRequest
ii-$*$ Query local ontology according to PolicyRule_ID
iii-$*$ Extract PolicyDecision
iv-$*$ Generate SecurityDecision
6-$*$ Generate SecurityDecisionBundle
7-$\leftharpoondown$ Send SecurityDecisionBundle to Policy Management (PM) service

5.2.5 Contextual Monitoring Service

Description: The Contextual Monitoring (CM) service is not strictly bound to the security architecture, since it serves multiple other actors and services including the quality of service (QoS) architecture. The functionalities of CMs relate to the maintenance of local awareness over the context under which the tactical nodes operate, including local and remote dynamic information, related to services, information, networks, radios, nodes and subjects. These information are collected locally through other services and by exploiting cross layer functionalities. Furthermore, entries in the CMs can be updated globally utilizing policy administration processes. It must be noted that CMs can also generate aggregated and statistical data for use within policy rules of limited priority. This allows the definition of simplified policy rules of limited computational complexity, for use under constrained network or local resources. For the two invocation cases initiated by the Security Handling (SH) service, the CMs only returns timely values of the

corresponding attributes. Yet, for the invocation initiated by the Metadata Handling (MH) service, the exact implementation of this process is system specific and can vary significantly in terms of the syntax, context or both, regarding the information transferred through the MH_UpdateResponse. In this sense, the generated MH_UpdateResponse may refer to a complete and updated policy copy or only the timely values of the dynamic data and object properties (In which case their incorporation occurs at the MHs, during inserting the ontological terminology and assertions Line 5 of MHs: functionalities).
Invocation: Invocation Originator $\Longrightarrow$ Invocation Form

1. Security Handling (SH) service $\Longrightarrow$ AttributeValuesRequest.
2. Security Handling (SH) service $\Longrightarrow$ CMsSnapshot_IDRequest.
3. Metadata Handling (MH) service $\Longrightarrow$ MH_UpdateRequest.

Functionalities: Internal=*, Input=$\rightharpoonup$, Output=$\leftharpoondown$

- For invocation type 1:
  1-$\rightharpoonup$ Receive AttributeValuesRequest from SHs
  2-$*$ Extract requested attributes
  3-$*$ Extract attribute values
  4-$*$ Generate AttributeValuesResponse
  5-$\leftharpoondown$ Send AttributeValuesResponse to SHs
- For invocation type 2:
  1-$\rightharpoonup$ Receive CMsSnapshot_IDRequest from SHs
  2-$*$ Extract timely value of 'ResourceAvailability' semantic
  3-$*$ Extract timely value of 'RefreshAlert' semantic
  4-$*$ Generate CMsSnapshot_IDResponse
  5-$\leftharpoondown$ Send CMsSnapshot_IDResponse to SHs
- For invocation type 3:
  1-$\rightharpoonup$ Receive MH_UpdateRequest from MHs
  2-$*$ Generate MH_UpdateResponse
  3-$\leftharpoondown$ Send MH_UpdateResponse to MHs

5.2.6 Policy Enforcement Point Service

Description: The Policy Enforcement Point (PEP) service operates as the output of the core security policy architecture towards the rest of the security or TSI services deployed in the processing pipeline. The role of the PEPs is to identify the service that provides the functionalities required for the enforcement of the policy decision, translate it to a suitable format for enforcement, and communicate it to the initial RequestorID.
Invocation: Invocation Originator $\Longrightarrow$ Invocation Form

1. Security Handling (SH) service $\Longrightarrow$ SecurityDecision.

2. Policy Management (PM) service $\Longrightarrow$ SecurityDecision.

Functionalities: Internal=*, Input=$\rightharpoonup$, Output=$\leftharpoondown$
1-$\rightharpoonup$ Receive SecurityDecision from SHs or PMs
2-$*$ Extract RequestorID from ActionRequestID
3-$*$ Generate ActionResponse
4-$\leftharpoondown$ Send ActionResponse to RequestorID

5.2.7 Functional Security Services

Additionally to the aforementioned core security architecture components, a variety of functional services can be incorporated in a modular manner through the TSI processing pipeline. These services refer to the enforcement of all the predefined protection goals (e.g. cryptography, management of digital certificates, access control, authentication, credential management, integrity protection, information labelling and filtering, security token management, provenance assurance).

In addition to some non security related services (e.g. packet queue, service registry, message session management), these functional security services are expected to invoke the extraction of policy decisions. Therefore, these services are assigned a RequestorID, and incorporate the appropriate interfaces towards the Security Handling service and from the Policy Enforcement Point service (denoted earlier as the singular ActionRequest and ActionResponse interfaces). These services can be defined following standardized processes. Yet, the developed architecture allows the incorporation of national and tailored solutions, satisfying the requirement for modularity towards the security enforcement mechanisms.

5.3 Test case based validation

As presented earlier, the designed TSI is targeted to the tactical domain. Thus the test cases used for the validation of the designed architecture were developed in accordance to common tactical operations, the experience gained from recent battlefields and the analysis of future requirements. The used tactical operations (e.g. Convoy, RSTA (Reconnaissance Surveillance and Target Acquisition), intervention patrol, MEDEVAC (Medical Evacuation), cordon and search, area denial) have been separated to specific use cases (e.g. Blue force tracking, COP distribution, injection of high mobility nodes, IED (Improvised Explosive Device) detection and report, interoperability with police forces) and detailed episodes (addressed request/ reply, multihop service invocation, service discovery, transitive service delivery, node isolation).

The communication between the defined core security services is achieved using SOAP messages, allowing the remote procedure call across the services. It is apparent that the service functionalities as presented earlier, correspond mainly to simple message modifications or substitutions. In this case a dedicated process receives a SOAP message (request) that contains all the required parameters, and transforms it into an invocation of the corresponding method. The resulting SOAP message (response) contains the required parameters for the continuation of the policy decision extraction process. Following this model, as presented in figure 5.3, an ActionRequest (according to its components) is mapped to a SecurityDecisionRequest by the Security Handling service. Consequently, the SecurityDecisionRequest (according to its components) is mapped to an ActionRequest_IDRepositoryEntry by the Policy Management service, while the process continues until the extraction of a valid ActionResponse towards the corresponding functional security service.

According to the results of our experiments, it is important to note that the complexity and dynamic adaptability of the developed mechanism is situated at the structure of the ontological knowledge base, the governing policy rules, the fine grained definition of action requests and the detailed incorporation of the available semantics, as described earlier [6, 3, 7, 4, 5]. Contrary to that, the functionalities of the presented core security services are kept at a low complexity level aiming for clear separation of duties within the policy decision extraction process. Thus, the identification of the appropriate SecurityDecisionRequest by the Security Handling service is a low complexity matching/querying process, despite of the fine-grained definition of security actions as a conjunction of the security domains (e.g protection, detection, diligence, response) and network capabilities (e.g. NCV-NATO Capability View).

The executed validation experiments highlighted the functionalities of the Metadata Handling service, and more precisely the reasoning phase (See: Metadata Handling Service / Functionalities/ 5.a.i to iv), as the process with most significant impact in terms of computational complexity within the policy decision extraction process. Aiming to counteract this obstacle and maintain the support of the required network functionalities, under a constrained operational status or across low capacity nodes, a variety of countermeasures have been deployed within the security policy mechanism, which are visible in the functionalities of the presented services.

- The Security Handling service can incorporate precomputed policy decisions, when this has been deemed necessary at the mission preparation stage.

- The Policy Management service utilises resource availability metrics at the prioritization of the ActionRequest_IDRepositoryEntries.

- The Policy Decision Point service connects each ActionRequest_ID to a PolicyRule_ID in accordance to resource availability metrics. Thus, for each reasoning cycle the complexity of the utilised policy rule depends on the locally available computational capacity. Additionally, as presented earlier, a default policy escape rule must be defined (across the prioritized dedicated rule stack) for each possible ActionRequest_ID for use under highly congested scenarios.
- The Metadata Handling service can incorporate supplementary reasoners (OWL, OWL Mini, OWL Micro) and instances of the local ontological knowledge base, for use under highly congested scenarios.
- Finally, a dedicated policy distribution mechanism has been developed [7], for the purpose of allowing the core security service architecture presented in this article, to be operable across the various platforms deployed within a tactical network.

5.4 Conclusions

Our research within the security aspects of TACTICS is tripartite. The first completed aspect was to analyse the requirements, validate, and recommend suitable controls and mechanisms for their attainment (e.g. recommendation of suitable solutions for the enforcement of the identified protection goals through the functional services). Consequently, the development of a suitable security policy framework, able to support and govern the functionality of the aforementioned mechanisms was required, and has been developed as presented earlier. The last major contribution towards a tactical SOA, has been presented in this article and relates to the design of a core security service architecture, able to instantiate the functionalities of the other two elements. The developed architecture provides configuration flexibility in a modular manner, while satisfying the defined requirements dynamically under varying network conditions. Additional SOA benefits include the information flow and performance improvement, maintaining the capacity to integrate existing or tailored assets, with reduced development and management cost. In our future work we intent to utilize our existing experimental results with the experience gained from the recent demonstration of the overall TACTICS TSI, towards the fine-grained adaptation of the developed mechanisms to the realistic conditions of contemporary areas of operations.

Acknowledgments

The results described in this work were obtained as part of the European Defence Agency project TACTICS (Tactical Service Oriented Architecture).

The TACTICS project is jointly undertaken by Patria (FI), Thales Communications & Security (FR), Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE (DE), Thales Deutschland (DE), Leonardo (IT), Thales Italia (IT), Norwegian University of Science and Technology (NO), ITTI (PL), Military Communication Institute (PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980.

Bibliography

[1] ALOISIO, A., AUTILI, M., D'ANGELO, A., VIIDANOJA, A., LEGUAY, J., GINZLER, T., LAMPE, T., SPAGNOLO, L., WOLTHUSEN, S. D., FLIZIKOWSKI, A., AND SLIWA, J. TACTICS: TACTICal Service Oriented Architecture. *CoRR abs/1504.07578* (2015). Available from: `http://arxiv.org/abs/1504.07578`. 43, 63, 103, 121, 143, 154, 189, 191, 212

[2] DIEFENBACH, A., GINZLER, T., MCLAUGHLIN, S., SLIWA, J., LAMPE, T. A., AND PRASSE, C. Tactics tsi architecture: A european reference architecture for tactical soa. In *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (May 2016), pp. 1–8. 63, 103, 121, 144, 155, 218

[3] GKIOULOS, V., AND WOLTHUSEN, S. D. Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks. *Norwegian Information Security Conference - NISK* (2015), 109–120. 43, 63, 103, 113, 122, 123, 143, 166, 168, 189, 191, 213, 218, 220

[4] GKIOULOS, V., AND WOLTHUSEN, S. D. Efficient security policy reconciliation in tactical service oriented architectures. In *International Conference on Future Network Systems and Security* (2016), Springer, pp. 47–61. 43, 63, 103, 113, 122, 123, 213, 223

[5] GKIOULOS, V., AND WOLTHUSEN, S. D. Securing tactical service oriented architectures. In *2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)* (July 2016), pp. 1–6. 63, 71, 103, 113, 122, 123, 143, 154, 157, 189, 191, 213, 218, 220

[6] GKIOULOS, V., AND WOLTHUSEN, S. D. A security policy infrastructure for tactical service oriented architectures. In *Conference on Security of Industrial-Control-and Cyber-Physical Systems* (2016), Springer, pp. 37–51. 63, 103, 104, 113, 122, 123, 213, 218, 220, 222

[7] GKIOULOS, V., AND WOLTHUSEN, S. D. *Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures*. Springer International Publishing, Cham, 2017, pp. 149–166. Available from: `http:`

//dx.doi.org/10.1007/978-3-319-44354-6_9. 43, 63, 103, 113, 114, 122, 123, 143, 189, 191, 213, 218, 223

[8] GKIOULOS, V., AND WOLTHUSEN, S. D. Security Requirements for the Deployment of Services Across Tactical SOA. *7th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security* (2017). 103, 213, 218, 220

[9] VASILEIOS, G., WOLTHUSEN, S. D., FLIZIKOWSKI, A., STACHOWICZ, A., NOGALSKI, D., GLEBA, K., AND SLIWA, J. Interoperability of security and quality of service policies over tactical soa. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)* (Dec 2016), pp. 1–7. 63, 103, 146, 214, 227

Chapter 6

Article 2b: Interoperability of Security and Quality of Service Policies Over Tactical SOA

Interoperability of Security and Quality of Service Policies Over Tactical SOA

2016 IEEE Symposium Series on Computational Intelligence (SSCI), Athens, 2016, pp. 1-7

Gkioulos, Vasileios Wolthusen, Stephen D.
Adam Flizikowski Anna Stachowicz Dariusz Nogalski
Kamil Gleba Joanna Sliwa

Abstract

Tactical networks are constrained networks that may transition between ad-hoc and mesh configurations and are characterised by frequent disruptions, changes in connectivity, and available resources. Whilst deploying a SOA allows the efficient provisioning of services at the tactical level, the existing resource limitations and potential attacks, require the dynamic adaptation of both QoS and security mechanisms. Within this environment, security and QoS must not only enforce the requisite functionalities, but also cooperatively seek optimal solutions for them according to their corresponding constraints and requirements. In this paper we propose a multi-domain policy-based decision subsystem supporting service delivery, that relies on an on-line knowledge-based reasoning mechanism. We describe the characteristics of such subsystem and show its benefits in relation to specific tactical requirements.

6.1 Introduction

Tactical C2 systems are used on contemporary battlefields in order to support the deployed assets fulfilling their corresponding tasks. During the mission execution stage, information and service delivery are of the highest importance. Such information may correspond to blue/ red force tracking or alerts, consolidating the required situational awareness. Moreover, where network provisioning allows, it is also desirable to offer access to higher echelons and more resource-intensive services. Current tactical communication

systems may operate over SatCom links with long latency on the order of several hundred millisecond, or wireless networks that may allow multi-MBit/ sec transfer rates but can also be limited to the low kBit/ sec range for some VHF waveforms, as well as be limited by spectrum contention and attacks. Additionally VHF networks may work with large jitter at the range of 9 seconds caused by channel access mechanisms. According to earlier experiments and field trials [22], the traffic load generated by C2 systems is very often too big for tactical communications systems. Therefore there is a strong need for an intelligent middle-ware layer that would adapt the user traffic, while at the same time supporting reliable and secure delivery of information under dynamic topology changes.

Further dynamic, but partially predictable changes to parameters including connectivity or route availability arise from interactions with node mobility and topography or channel reservation. This is particularly challenging for SOA, as service invocations may span multiple nodes in a given transaction, and where some underlying wireless networks may impose long queues and do not allow for rapid message acknowledgements. Service and message prioritisation is therefore a key aspect of enforcing QoS constraints, where invocations or messages to avoid jeopardising lives and mission objectives must take precedence over optimal network utilisation for multiple competing services.

These challenges are addressed by the EDA TACTICS [3] project, by proposing a SOA-based middle-ware (so called TSI), supporting information distribution on the tactical level. The designed TSI [9] consists of several core services, the configuration and composition of which is to support information delivery. This is however a very complicated task that must take into account the command structure, mission objectives, current situation on the battlefield, and risk of releasing vulnerable information to the enemy while maximizing overall mission effectiveness. The overall TSI configuration is a complicated task that cannot be statically predefined.

In public communication systems, the network infrastructure is commonly over-provisioned, giving the possibility to support traffic overload levels that have been predicted in the system planning phase. Communication systems at the battlefield cannot support even those standard information relations due to their generic low capacity. Thus, within TACTICS the problem of traffic adaptation is critical. However, limiting the traffic size may require the necessity to modify and shape it, taking into account its priority and the specific requirements of the mission. The military background of TACTICS makes it also necessary to consider the security and reliability dimension of information relations. Some messages must be delivered intact or must be secured (e.g. encrypted, protected from integrity loss) due to the life preservation requirement. Yet, these two concepts may be contradictory given the limited bandwidth of tactical networks. This problem is not

common in public networks, but in tactical networks it becomes the main issue very often forgotten in research. The TSI configuration requires that all TSI core services are assigned actions that must be performed in sequence, for the middle-ware to work efficiently under a given set of conditions.

Whilst some parameters and choices can be configured during the mission preparation stage, many will become known only during the mission itself and must hence be responded to dynamically. We therefore argue that a policy-based mechanism capable of incorporating situational context and decisions is desirable for tactical networks middle-ware control. Having previously demonstrated the effectiveness of such on-line reasoning mechanisms for adapting decisions over security policies [12, 16, 13, 14, 15] and research results on system-to-system mediation by overcoming structural domain differences [26, 25, 24], in this paper we propose a security and QoS interoperability mechanism.

This article focuses on the problem of the QoS and security domains interoperability as it has been studied in the EDA TACTICS project. Interoperation between TACTICS decision domains refers to achieving an agreed decision via trade-offs between the QoS and Security domain controllers. We highlight the selected TACTICS QoS and security requirements, and present the developed decision subsystem architecture. The control logic (context dependent rules) to conduct adaptations will be subject to following research (validation step). Hereby we only present a simple integration example according to the designed tactical service infrastructure. The remainder of this paper is structured as follows: Section 6.2 presents related work in the corresponding areas. Sections 6.3 and 6.4 present individual and complementary aspects of the topic under the scope of security and QoS, based on our earlier studies. Sections 6.5, 6.6, and 6.7 provide an overview of the designed solutions, referring to the decision subsystem, policy framework and interoperability mechanism.

6.2 Related work

The dynamic orchestration of services has been known to be a hard problem, Yu et al. demonstrated that even for a static configuration, selecting optimal services, whether for QoS, security, or both, is an NP-hard problem [34]. Subsequent work such as by Nejdl et al. investigated further heuristic approaches [4] where Ben Mabrouk et al. proposed the use of a guided heuristic for dynamic service composition [7] whilst Li et al. proposed a QoS-based composition, tolerating random faults via case-based reasoning [19]. The authors are not aware of work explicitly covering dynamic networks such as tactical networks with existing work focusing on near-optimal selection of end-to-end QoS, which may not be possible in a highly dynamic tactical network where decisions may be required also locally [21]. However, Al-

Ridhawi and Karmouch recently proposed a semantically-oriented per-hop approximation of service composition that is applicable to mobile networks [1]. Similar considerations as for composition also apply to QoS- aware service discovery [20] even where service registries are largely static as may be the case for configurations set up at the mission preparation stage in tactical networks.

Ontological models for describing QoS characteristics have also been studied building for example on the DARPA Agent Markup Language-Service (DAML) [36] for service discovery in early work; a more recent survey and analysis is provided by Zeshan et al. [35]. Similar works aimed to enhance web service discovery/ selection [28, 11, 2, 10, 32] and composition [5, 33]. Yet, facets such as ontology-based approach for QoS monitoring and QoS adaptation in SOA systems even if mentioned, are not thoroughly investigated.

Similar efforts have also focused on adding security metadata and capabilities to service descriptions such as the NRL Security Ontology by Kim et al. [17] as the WS-Security Policy standard does not offer explicit semantics; this has led to efforts such as work by Di Modica and Tomarchino to augment WS-Policy documents [8] and more recently efforts to map these into an OWL-DL ontology by Ben Brahim et al. [6]. Our earlier work [12, 16, 13, 14, 15] has described capturing security properties and objectives for the dynamic modelling and evaluation of security policies in the form of ontologies over which a description logic fragment can be used for on-line, distributed reasoning. However the work concentrated mainly on security measures and policies, and further research is needed on how such an approach can fit into a combined QoS and Security policy framework.

Interoperability in military systems [31, 30, 18, 26, 25, 24, 29] can refer to the physical [27] (interoperability of radio communication), syntactical [23] (common data modelling) or semantic level [25] (ability of two computerized systems to exchange information for a specific task and make sure that the meaning of the information is accurately and automatically interpreted by the receiving system). The role of a knowledge-based C2 system mediator is to solve the conceptual mismatch problem knowing the context under which the two systems interoperate and the common operational goal. The research however does not address the tactical wireless network constraints but rather higher levels of commands where network problems are reduced.

It is evident that earlier work focused on the incorporation of limited security related aspects within developed QoS frameworks and conversely. Yet, the attainment of the required functionalities within tactical networks requires a mechanism dedicated to the consolidation of the unique and domain specific requirements, given the underlying constraints.

6.3 Constraints and Requirements

The security and QoS requirements must be satisfied both pro-actively and reactively. An ontological representation does not permit contradictions within a common knowledge base; however, conflicting objectives among QoS and security are inevitable and must be kept representationally disjoint.

6.3.1 Security Related Considerations

As shown earlier, requirements for security of individual and composed services refer both to fundamental protection goals (such as confidentiality, integrity, availability) and layered requirements (such as non-repudiation, labelling, traceability) referring to transmitted or data at rest and the processing procedures constituting the service delivery. For that purpose, the security mechanisms must be scalable and should incorporate information from various layers of the SOA platform. Such cross-layer information can become visible and be utilised within the defined security policies, in order to support their dynamic adaptation to the continuous network alterations. Additionally, the functional constraints of tactical nodes require the adaptation of the implemented security mechanisms, in order to support both isolated and cooperative operation. In the context of dynamic adaptation, this partitioning capability can allow the partial or complete delegation of security related functionalities across the deployed actors, provided that stand-alone operability is maintained.

6.3.2 QoS Related Considerations

Although a large body of knowledge relevant to QoS can be configured in the mission preparation stage such as service types and priorities or node capabilities including radios and mobility, dynamic adaptation plays a larger role. For some services, such as blue force tracking, it will be possible to configure the maximum delay for which such messages can be queued, diverted, or be put on hold before discarding, while maintaining sufficiently frequent updates to retain a situational picture. Similarly, certain types of messages and service invocations such as MEDEVAC requests must be prioritised. Reasoning and decisions over QoS in tactical networks must occur at several levels from radio frequency interface selection and message queueing, via route selection and service invocation, up to service semantics where e.g. service substitution may need to occur. QoS mechanisms frequently rely on discovery of available resources and services, and will use explicit resource reservation to enforce requirements and constraints. Yet, given the limitations of tactical networks this would require allocation of a substantial fraction of all available resources to the QoS infrastructure. Instead, we argue that QoS mechanisms for tactical networks can only rely

on implicitly available information obtained from the local node. This information such as on routing or channel characteristics, including latency and packet loss rate, is gathered in the knowledge base from several abstraction layers, however, and only in rare instances can this be augmented by a node-external query. A key requirement, moreover, is that the adaptation mechanism is itself sufficiently agile that decisions for selecting services or their configuration occur in a timely manner before the configuration of the tactical network changes and thereby invalidates the evaluated configuration.

6.4 Interoperability Requirement

The interoperability requirement between the security and QoS mechanisms results from the aforementioned distinction of priorities and motivation, which at times may impose contradictory objectives. Furtheremore, equally important is the notion of policy dynamicity, which refers to the on-line adaptation of security and QoS policies due to alteration of contextual parameters. QoS aims to adapt the traffic flow (user traffic and TSI outgoing traffic) to fit into the limited communication channel, maximizing resource utilization by the user data. Concurrently, security aims to guarantee the enforcement of corresponding protection goals, such as privacy, integrity, authentication, authorization and intrusion detection. This however comes with a price of additional overhead, that leads to resource deprivation from the transmission of plain user data. Thus the aim of security and QoS interoperability is to reach a common agreement given the highest good-put and the optimum denominator in terms of security measures.

If for a given action (e.g. service invocation) the cumulative security and QoS overhead exceeds the available channel bandwidth, an alternative solution must be negotiated, referring either to action substitution (e.g. service substitution) or action parametrization (e.g. routing/ encryption algorithm replacement). This may be the case when it is necessary to enforce lighter security mechanisms (e.g. shorter key length or selection of pre-shared symmetric keys instead of key negotiation), or shape user data (e.g. message payload reduction or message drop). Even in the simplified scenario of a routing decision request from a deployed Messaging_service to the Routing_service, the getNextHop() admission has distinct policy requirements for QoS and security.

In a more specific scenario though, if the message is already protected by integrity mechanisms, it cannot be modified without breaking message integrity. Thus, payload reduction must be removed from the available adaptations. In another scenario of interoperability goals, QoS aware routing should be enriched with intrusion detection information for the avoidance of compromised nodes, based on dynamic trust management information.

Additionally, the selected QoS and security related actions must be prioritised (e.g. message modification before integrity and encryption).

Thus, the interoperability requirements should be achieved, while security and QoS maintain their corresponding decision focus, allowing transparency for the reconciliation of their distinct decisions. This reconciliation is to occur in a small number of discrete steps allowing partial re-use of reasoning structures, where each domain must apply pre-configured relaxations until requirements are satisfied or an empty resolution is obtained.

6.5 TACTICS TSI and Decision Subsystem

The overarching goal of TACTICS is to define the reference architecture of the TSI, as a middle-ware placed between the IS (Information System) and the radio, transparently given the utilization of standard tactical radio equipment. The TSI concept architecture divided the middle-ware into two vertical stacks, as presented in figure 6.1. The Controller holds the whole intelligence and supervises the functionality of particular processing layers of the TSI. The second acts as the Processing Pipeline, which processes messages coming from the IS down to the bearer (radio access level) at three horizontal layers, namely Service, Message and Packet.

The Processing pipeline handles sessions, processes messages, cuts them into packets and sends them out through the radio (or other network interfaces). Each of the three layers has means to enforce QoS mechanisms adapting the traffic to the current network conditions and device status, as well as security mechanisms supporting confidentiality, integrity and access control (so called PEP, Policy Enforcement Point). These mechanisms are triggered by actions, the activation of which is decided in the Controller (see chapter 6.7). The Controller collects the aforementioned cross-layer information and on the basis of that, enforces policies which configure the Processing Pipeline. Such an approach makes the controlling process independent of singular messages coming to the TSI node. Thus, the PEPs are governed by the policies defined within the Controller referring to security and QoS mechanisms on the particular level. It is worth mentioning that the Controller is able to continuously adapt its decision-making process based on the feedback received through the cross-layer information, after the completion of an action (e.g. successful message transmission or deletion, intrusion detection etc)

6.6 Ontology and Policy Framework

The distinct security and QoS domains and capabilities can be defined as a cohesive group of elements (e.g. enforcement mechanisms, observable objects and actions) aiming to the fulfilment of the aforementioned discrete

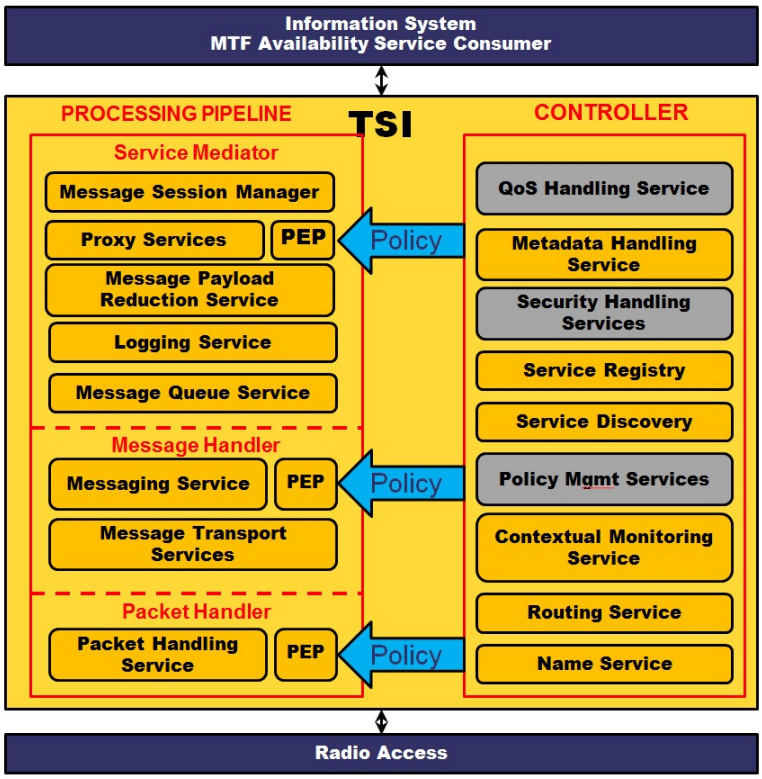

Figure 6.1: Processing pipeline and controller in the TSI architecture.

goals. Each domain is responsible for the collection of subset environmental parameters, and the management of suitable enforcement mechanisms by taking decisions from its own perspective, for the governance of required actions. Each domain is branched into corresponding sub-domains (e.g. Security - protection, detection, diligence, planning, response // QoS - resource reservation, congestion management, traffic admission, service level agreements). Even though TACTICS requires from each domain to maintain its own decision focus, both QoS and Security may impact each other and enforce contradictory decisions. TACTICS harmonizes both decisions under the frame of a common interoperability goal.

This chapter gives basis to the formal definition of a TACTICS common policy model, in the sense that such policy model should support a multi-domain decision environment. The policy model should be comprehensive enough to allow negotiation/ deconflictation of QoS and Security cross-layer decisions. Equally important is the notion of policy dynamicity,

which refers to the on-line adaptation of security and QoS policies due to alteration of contextual parameters. The notion of dynamicity is incorporated across two distinct dimensions. Initially, the use of ontological structures facilitates the refined capturing of dynamic attributes, across a detailed description of the deployed tactical system in a distributed, prioritized and aggregated manner. Additionally, the alterations of such dynamic attributes is addressed not only by their monolithic incorporation across policy decisions, but in a layered manner by the definition of prioritized rule-sets for each of the expected actions/ interoperability goals.

In respect to the observable objects, each domain is responsible for the collection of subset environmental parameters, for the population of the local knowledge base. The TACTICS common ontology is defined as a knowledge base, where the T-Box is a set of classes, properties and axioms, while the A-Box is a set of individual terms and assertion sentences. The T-Box terms are divided into three basic sets, namely Core, QoS and Security, where:
Core: Elements related to common and generic classes, such as:

- User
- Service
- Device
- Radio network
- Information
- Topology

and properties, such as:

- Service invokes service
- Service is deployed on device
- Network is accessed by user
- Network uses radio
- User accesses network
- Device is located at

Each of these elements within the core is further specialized. Thus, Core: Information may be specialized as Core: - Message and further as Core: - User - Message or Core: - Signalling - Message. Similarly the security and QoS sets are constructed, according to the corresponding domain specific requirements, as presented at figure 6.2. It must be noted that the construction and deployment of the defined policies is conducted at the mission preparation stage, where no computational or other constraints are present. At this stage optimal solutions are approximated with the incorporation of mission specific operational requirements and the use of computational intelligence methods.

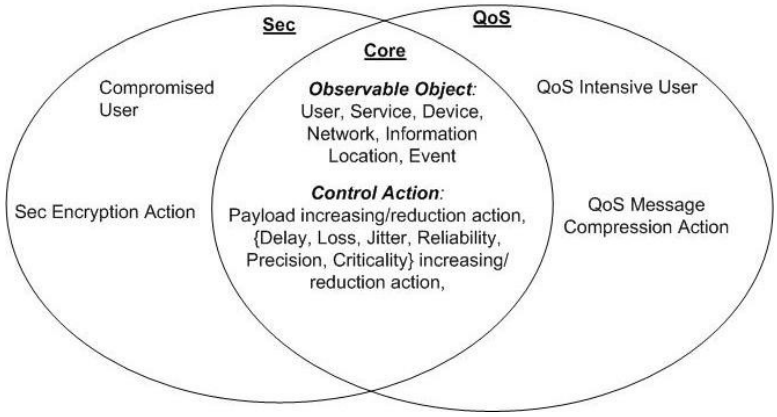

Figure 6.2: Simplified example of multi-domain ontology construction.

The aforementioned enforcement mechanisms refer to security and QoS dedicated services, capable of enforcing the policy decisions in respect to the questioned actions. The defined enforcement mechanisms include, but are not limited to:

- Session manager
- Service registry
- Message queue
- Trust management
- Encryption
- Intrusion detection
- Service choreography
- Routing
- Traceability
- Message adaptation

6.7 Interoperability of Security and QoS

The TRA (Tactical Service Infrastructure Reference Architecture) created within TACTICS, has been modelled in accordance to the NATO Architecture Framework 3.1. The elements of the TSI architecture aiming to facilitate the interoperability of security and QoS mechanisms are:
Action requester: A service that initiates an action request. It can be either the Security Handler or the QoS Handler, which monitoring network parameters identify the requirement for a specific action/ adaptation. Each of these elements can additionally incorporate precomputed or generic policy decisions, which are enforced by the corresponding PEPs without invoking the Policy Manager. This mechanism is integrated for optimization purposes in case or constrained reasoning resources.
Security/ QoS PEP: A service that incorporates the required mechanisms

or knowledge, for the enforcement of any generated or precomputed policy decision.
Policy manager: A service that transfers the decision request to the Security/ QoS Policy Decision Points and the Metadata Handler. Additionally, the policy manager is responsible for the deconflictation of the PDPs decisions.
Security/ QoS PDP: A service that contains the policy rules for the available action requests for instance identification. Multiple rules are constructed for each action request, incorporating static and dynamic attributes regarding services, information, nodes, radios, networks and subjects. The rules corresponding to each action request, are prioritized and utilized for deconflictation purposes between the security and QoS domains.
Metadata Handler: An ontologically constructed knowledge-base that incorporates static and dynamic attributes required for policy decisions. These attributes may refer to services, information, nodes, radios, networks and subjects. Metadata Handler constructs a static copy of the ontological structure (snapshot) at the initiation of an access request, which is maintained until the successful generation of a valid/ deconflicted policy decision. Reasoning for a given action request is achieved with the use of this dedicated static copy and the policy rules included at the PDPs
Contextual monitoring: A service that periodically monitors the dynamic attributes, while it also incorporates mechanisms for the computation of statistical and aggregated values. These attributes are incorporated into policy rules, for optimization purposes in cases or constrained reasoning resources.

6.7.1 Analytical scenario

The interconnectivity of the defined elements is presented at figure 6.3, while the functionalities of the numbered interactions can be described with the use of a simplified message prioritization scenario. Assuming that a message labelled as *"Alert"* arrives at the Message Queue (MQ), the MQ operating as action solution requester transfers an Action Solution Request (ASR) to the QoS Handler (QH). Concurrently the following functionalities occur, as depicted at figure 6.3.

- **Functionality 1, Interaction 1:** QH seeks locally stored precomputed solution in cooperation with the Security Handler (SH), to be transferred directly for enforcement to QoS PEP. (For the purpose of the scenario, no solution if found at this stage. If a precomputed solution is found at this stage, the procedure is completed successfully.)

- **Functionality 2, Interaction 2:** QH requests ASR dedicated snapshot of Metadata Handler (MH) at time T0. This message initiates the AReS (Action Request Session) with a dedicated Action Request Session ID (AReS.ID).

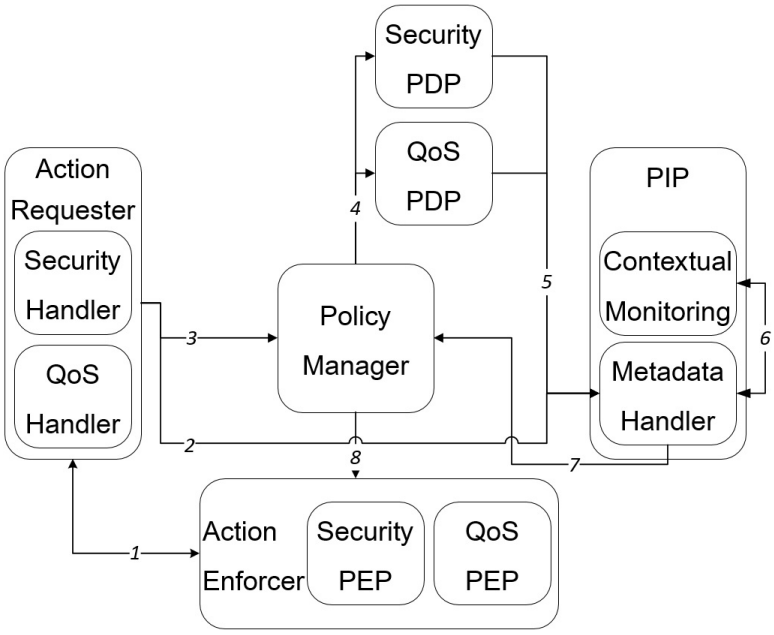

Figure 6.3: Elements and flows involved into policy decisions.

- **Functionality 3, Interaction "Self":** QH locally resolves the ASR, generating QoS oriented list of prioritised Action Solutions (AS).
  - Note 1: AS computation is based on partial information (e.g. limitations of routing protocol)
  - Note 2: Computation at the level of the Action Requester (AR) may rely on lookup tables, partial knowledge bases, or algorithmic solutions which are defined at the mission preparation stage.
  - Note 3: The computed AS refer to the message type of the examined message, based on predefined attributes and has the prioritised form:
    AS1 = MessageTypeX.priority(High)
    AS2 = MessageTypeX.priority(Medium).
- **Functionality 4, Interaction 3:** QH transfers an Action Request (ARe) to the Policy Manager (PM). The ARe is formed as a bundle, including the optimal AS and the dedicated AReS.ID, which is bound to the dedicated MH snapshot.
  - Note 1: There is an one to one mapping between the ARes.ID and the Snapshot ID (Sn.ID)

  - Note 2: ARe has the form: ARe=(AReS.ID, AS1)

- **Functionality 5, Interaction 4:** PM transfers the ARe to the security and QoS PDPs.

- **Functionality 6, Interaction "Self":** The two PDPs identify the dedicated sets of rules for the examined ARe (MessageTypeX, prioritization), based on their decision contexts and the common interoperability goal.

  - Note 1: The rules are in the form of prioritized queries.
  - Note 2: Identification is achieved with the use of lookup tables, which are constructed at the mission preparation stage.

- **Functionality 7, Interaction 5:** The set of first priority rules (one from security and one from QoS) are transferred to the MH. The messages carry the predefined AReS.ID as:
  QoS: (AReS.ID, QoS_Rule1)
  Security: (AReS.ID, Security_Rule1)

- **Functionality 8, Interaction 6:** MH reasons for the examined session, given the session dedicated copy of the ontology (Sn.ID) and the received set of rules. The MH returns:
  Allow acknowledgement: If instances have been identified on a query.
  Not allow acknowledgement: If no instances have been identified.

- **Functionality 9, Interaction 7:** MH transfers the query responses to the PM.

- **Functionality 10, Interaction 8:** PM evaluates the responses and if they are not contradictory AS1 is transferred to the QoS PEP for enforcement. Possible contradictions are resolved with the use of the aforementioned deconflictation mechanisms (In a least constrained scenario, this can be achieved with an examination of secondary rules and AS).

6.8 Conclusion

The attainment of interoperability across the security and QoS requirements of constraint tactical networks imposes multiple challenges. Under this scope, this article presents the designed mechanisms for that purpose, within the project TACTICS. The identified constraints and requirements have been presented along with the architecture of the decision subsystem. Additionally, an insight has been provided over the utilised ontology and policy framework, focusing on the developed interoperability mechanism. Our

future work will focus on the refinement of the presented framework, according to the requirements of tactical networks.

Acknowledgements

The results described in this work were obtained as part of the EDA project TACTICS. The TACTICS project is jointly undertaken by Patria(FI), Thales Communications & Security(FR), FKIE(DE), Thales Deutschland(DE), Leonardo(IT), Thales Italia(IT), NTNU(NO), ITTI(PL), MCI(PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980.

Bibliography

[1] AL RIDHAWI, Y., AND KARMOUCH, A. Decentralized Plan-Free Semantic-Based Service Composition in Mobile Networks. *IEEE Transactions on Services Computing 8*, 1 (Jan./Feb. 2015), 17–31. 123

[2] ALNAHDI, A., LIU, S.-H., AND MELTON, A. Enhanced Web Service Matchmaking: A Quality of Service Approach. In *IEEE World Congress on Services (SERVICES)* (2015), IEEE, pp. 341–348. 123

[3] ALOISIO, A., AUTILI, M., D'ANGELO, A., VIIDANOJA, A., LEGUAY, J., GINZLER, T., LAMPE, T., SPAGNOLO, L., WOLTHUSEN, S. D., FLIZIKOWSKI, A., AND SLIWA, J. TACTICS: TACTICal Service Oriented Architecture. *CoRR abs/1504.07578* (2015). Available from: `http://arxiv.org/abs/1504.07578`. 43, 63, 103, 121, 143, 154, 189, 191, 212

[4] ALRIFAI, M., RISSE, T., DOLOG, P., AND NEJDL, W. A Scalable Approach for QoS-Based Web Service Selection. In *Proceedings of the Fourth International Workshop on Engineering Service-Oriented Applications (ICSOC 2008)* (Sydney, Australia, Dec. 2009), G. Feuerlicht and W. Lamersdorf, Eds., vol. 5472 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 190–199. 122

[5] BACCAR, S., ROUACHED, M., AND ABID, M. A user requirements oriented semantic web services composition framework. In *IEEE Ninth World Congress on Services (SERVICES)* (2013), IEEE, pp. 333–340. 123

[6] BEN BRAHIM, M., CHAARI, T., BEN JEMAA, M., AND JMAIEL, M. The SemSPM Approach: Fine Integration of WS-SecurityPolicy Semantics to Enhance Matching Security Policies in SOA. *Service Oriented Computing and Applications 10*, 1 (Feb. 2016), 1–28. *(in press)*. 123

[7] BEN MABROUK, N., BEAUCHE, S., KUZNETSOVA, E., AND NIKOLAOS GEORGANTAS, V. I. QoS-Aware Service Composition in Dynamic Service Oriented Environments. In *Proceedings of the 2009 10th International ACM/IFIP/USENIX Middleware Conference (Middleware 2009)* (Urbana-Champaign, IL, USA, Dec. 2009), J. M. Bacon and B. F. Cooper,

Eds., vol. 5896 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 123–142. 122

[8] DI MODICA, G., AND TOMARCHINO. Semantic Security Policy Matching in Service Oriented Architectures. In *Proceedings of the 2011 IEEE World Congress on Services* (Washington D.C., USA, July 2011), D. S. Milojicic and M. Kirchberg, Eds., IEEE Press, pp. 399–405. 123

[9] DIEFENBACH, A., GINZLER, T., MCLAUGHLIN, S., SLIWA, J., LAMPE, T. A., AND PRASSE, C. TACTICS TSI architecture: A European reference architecture for tactical SOA. In *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (May 2016), pp. 1–8. 63, 103, 121, 144, 155, 218

[10] DOBSON, G., AND SANCHEZ-MACIAN, A. Towards unified QoS/SLA ontologies. In *Services Computing Workshops IEEE* (2006), IEEE, pp. 169–174. 123

[11] DUYGU ÇELIK, A. A. E. Ontology-Based QoS Queuing Model for Selection of Web Services Servers. In *IEEE 34th Annual Computer Software and Applications Conference Workshops (COMPSACW)* (2010), IEEE, pp. 7–12. 123

[12] GKIOULOS, V., AND WOLTHUSEN, S. D. Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks. *Norwegian Information Security Conference - NISK* (2015), 109–120. 43, 63, 103, 113, 122, 123, 143, 166, 168, 189, 191, 213, 218, 220

[13] GKIOULOS, V., AND WOLTHUSEN, S. D. Efficient security policy reconciliation in tactical service oriented architectures. In *International Conference on Future Network Systems and Security* (2016), Springer, pp. 47–61. 43, 63, 103, 113, 122, 123, 213, 223

[14] GKIOULOS, V., AND WOLTHUSEN, S. D. Securing tactical service oriented architectures. In *2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)* (July 2016), pp. 1–6. 63, 71, 103, 113, 122, 123, 143, 154, 157, 189, 191, 213, 218, 220

[15] GKIOULOS, V., AND WOLTHUSEN, S. D. A security policy infrastructure for tactical service oriented architectures. In *Conference on Security of Industrial-Control-and Cyber-Physical Systems* (2016), Springer, pp. 37–51. 63, 103, 104, 113, 122, 123, 213, 218, 220, 222

[16] GKIOULOS, V., AND WOLTHUSEN, S. D. *Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures*. Springer International Publishing, Cham, 2017, pp. 149–166. Available from: `http://dx.doi.org/10.1007/978-3-319-44354-6_9`. 43, 63, 103, 113, 114, 122, 123, 143, 189, 191, 213, 218, 223

[17] KIM, A., LUO, J., AND KANG, M. Security Ontology to Facilitate Web Service Description and Discovery. In *Journal on Data Semantics IX* (Heidelberg, Germany, July 2007), S. Spaccapietra, P. Atzeni, F. Fages, M.-S. Hacid, M. Kifer, J. Mylopoulos, B. Pernici, P. Shvaiko, J. Trujillo, and I. Zaihrayeu, Eds., vol. 4601 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 167–195. 123

[18] LEVENSHTEYN, R., AND FIKOURAS, I. Mobileman: design, integration, and experimentation of cross-layer mobile multihop ad hoc networks. *IEEE Communications Magazine 44*, 7 (July 2006), 80–85. 123

[19] LI, G., LIAO, L., SONG, D., AND ZHENG, Z. A Fault-Tolerant Framework for QoS-aware Web Service Composition via Case-Based Reasoning. *International Journal of Web and Grid Services 10*, 1 (Jan. 2014), 80–99. 122

[20] LIN, D., SHI, C., AND ISHIDA, T. Dynamic Service Selection Based on Context-Aware QoS. In *Proceedings of the IEEE Ninth International Conference on Services Computing (SCC 2012)* (Honolulu, HI, USA, June 2012), L. Moser, M. Parashar, and P. Hung, Eds., IEEE Press, pp. 641–648. 123

[21] LIN, S.-C., AND CHEN, K.-C. Cognitive and Opportunistic Relay for QoS Guarantees in Machine-to-Machine Communications. *IEEE Transactions on Mobile Computing 3*, 1 (Mar. 2016), 599–609. 122

[22] MANSO, M., CALERO, J. M. A., BARZ, C., BLOEBAUM, T. H., CHAN, K., JANSEN, N., JOHNSEN, F. T., MARKARIAN, G., MEILER, P.-P., OWENS, I., ET AL. SOA and Wireless Mobile Networks in the tactical domain: Results from experiments. In *Military Communications Conference, MILCOM 2015-2015 IEEE* (2015), IEEE, pp. 593–598. 121, 214

[23] MIP. Joint Command and Control Information Exchange Data Model, 2014. Available from: `https://mipsite.lsec.dnd.ca/Pages/Default.aspx`. 123

[24] NOGALSKI, D., FORD, R., KUEHNE, S., HANSEN, B.-J., HANZ, D., LAST, M., MOJTAHEDZADEH, V., SANTOS, L., TUNCER, F., AND WUNDER, M. Bridging Semantic Interoperability gaps with SILF. In *International Conference on Military Communications and Information Systems (ICMCIS)* (May 2015), pp. 1–11. 122, 123

[25] NOGALSKI, D., FORD, R., KUEHNE, S., HANSEN, B.-J., HANZ, D., LAST, M., MOJTAHEDZADEH, V., SCAMARCIO, G., TUNCER, F., AND WUNDER, M. Framework for Semantic Interoperability. Tech. Rep.

STO-TR-IST-094 AC/323(IST-094)TP/525, NATO Science and Technology Organisation, 2014. Reference STO-TR-IST-094 AC/323(IST-094)TP/525. 122, 123

[26] NOGALSKI, D., AND NAJGEBAUER, A. Semantic mediation of NATO C2 systems based on JC3IEDM and NFFI ontologies. In *NATO RTO symposium on Semantic and Domain based Interoperability* (November 2011). Reference RTO-MP-IST-101 AC/323(IST-101)TP/426. 122, 123

[27] NSO. STANAG 5066 C3B (Edition 3) - Profile for HR radio data communications, March 2015. 123

[28] QU, L.-L., AND CHEN, Y. QoS ontology based efficient web services selection. In *International Conference on Management Science and Engineering (ICMSE)* (2009), IEEE, pp. 45–50. 123

[29] SEYMER, P., STAVROU, A., WIJESEKERA, D., AND JAJODIA, S. QoP and QoS policy cognizant module composition. In *IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY)* (2010), IEEE, pp. 77–86. 123

[30] SRIVASTAVA, V., AND MOTANI, M. Cross-layer design: a survey and the road ahead. *IEEE Communications Magazine 43*, 12 (Dec 2005), 112–119. 9, 123

[31] TOLK, A., AND MUGUIRA, J. The Levels of Conceptual Interoperability Model (LCIM). In *Proceedings of the Fall Simulation Interoperability Workshop* (2003). 123

[32] XUAN, V. WS QoSOnto: a QoS ontology for web services. In *IEEE International Symposium on Service-Oriented System Engineering, (SOSE)* (2008), IEEE, pp. 233–238. 123

[33] YANG, H., CHEN, X., AND LIU, S. Research and implementation on QoS ontology of web service-oriented composition. In *2nd International Symposium on Information Engineering and Electronic Commerce (IEEC)* (2010), IEEE, pp. 1–4. 123

[34] YU, T., ZHANG, Y., AND LIN, K.-J. Efficient Algorithms for Web Services Selection with End-to-End QoS Constraints. *ACM Transactions on the Web 1*, 1 (May 2007), 1–26. 122

[35] ZESHAN, F., MOHAMAD, R., AND AHMAD, M. N. Quality of Service Ontology Languages for Web Services Discovery: An Overview and Limitations. In *Proceedings of the 15th International Conference on Human Interface and the Management of Information (HCI International 2013)* (Las Vegas, NV, USA, July 2013), S. Yamamoto, Ed., vol. 8016 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 400–407. 123

[36] ZHOU, C., CHIA, L.-T., AND LEE, B.-S. Web Services Discovery with DAML-QoS Ontology. *International Journal of Web Services Research 2*, 2 (Apr. 2005), 43–66. 123

Chapter 7

Article 3a: A Security Policy Infrastructure for Tactical Service Oriented Architectures

A Security Policy Infrastructure for Tactical Service Oriented Architectures

Conference on Security of Industrial-Control and Cyber-Physical Systems (CyberICPS), Heraklion, 2017, Springer, LNCS, volume 10166, pp. 37-51.

Gkioulos, Vasileios Wolthusen, Stephen D.

Abstract

Tactical networks are affected by multiple constraints related to the limited node characteristics and the availability of resources. These constraints within the highly dynamic tactical environment, impose significant limitations to the functionalities and efficiency of current generic security policy frameworks.

Earlier studies have provided a risk analysis of tactical SOA, and a set of fine-grained protection goals in correspondence to the aforementioned constraints. Furthermore, web ontology language has been identified as a suitable mediator towards the requirements and opportunities imposed by tactical SOA. Thus, in this article we present a security policy framework dedicated to tactical networks, as it has been developed within the project TACTICS.

7.1 Introduction

Tactical networks are of Ad-Hoc nature, subjected to a variety of constraints related both to the limited operational characteristics of the deployed nodes and the scarcity of network resources. Such constraints impede the attainment of requisite protection goals, by rendering current generic solutions unsuitable, due to limited adaptability over the network dynamics. For that purpose, within the project TACTICS, suitable security solutions have been developed, tailored to the characteristics of tactical service oriented architectures. Within this scope our study aims to identify and support fine-grained protection goals over the initial over provisioned operational stages, but

mainly through the anticipated degraded and disrupted mission execution phases.

Earlier studies [9, 1] presented a detailed risk analysis of tactical SOA, investigating the impact of the aforementioned constraints across the three stages of tactical operations (preparation-execution-debrief). Furthermore, suitable security requirements and protection goals have been identified, referring to the security of communication procedures, transitive information, data at rest and service choreography related processes. Finally, the feasible benefits of exploiting the unique characteristics of service oriented architectures have been identified, aiming to utilise them for the enhancement of the implemented security mechanisms.

The results of these studies have been consequently utilised for the extraction of functional requirements in respect to the developed security policy mechanisms [8, 10]. These requirements include constraints related to scalability, real time dynamic adaptability, cross layer implementation and distributed deployment. A parallel evaluation between the identified functional policy requirements and the constraints imposed by the nature of tactical SOA, was undertaken for the examination of suitable security policy frameworks. This examination included commonly used mechanisms, such as WS-Security, SAML[16], XACML[17] and Ponder[5], as well as recent semantic (REI [11], KAOS [19], ROWLBAC [7], Kolter et al. [12], Trivellato et al. [18]) and trust management frameworks (cassandra [3], Tulip [4], RT [13], Peer-Trust [15]). This analysis promoted the use of web ontology language as the most suitable solution in respect to the requirements of tactical SOA. Thus, the same study presented a tactical policy framework and our initial results regarding its conceptualisation.

In this paper we present a detailed analysis of this security policy framework dedicated to tactical SOA, as it has been designed within TACTICS. Section 7.2 introduces the developed tactical service infrastructure, focusing on the security related services, their interactions and functionalities. Section 7.3 presents the core policy model in accordance to the decision process, along with the required steps for the policy formalization. Finally, section 7.4 includes a simplified example of the prototype implementation developed for validation and demonstration purposes.

7.2 Tactical Service Infrastructure-TSI

Four distinct instances of tactical nodes have been assumed within TACTICS, each of whom supports the delivery of a defined associated functionality set, through standard interfaces. The studied tactical node types are:

- TSI Node-Dismounted: Carried by individual soldiers.
- TSI Node-Mobile: Integrated in single vehicles.

- TSI Node-HQ: Integrated in semi-permanent headquarters.
- TSI Node-Custom: Unmanned operational node.

The internal TSI components along with a subset of the defined core functionalities are presented at figure 7.1, while the security related services are highlighted (yellow). The middle-ware has been divided into two vertical stacks, as it was presented in detail by Thorsten et al. [6] namely:

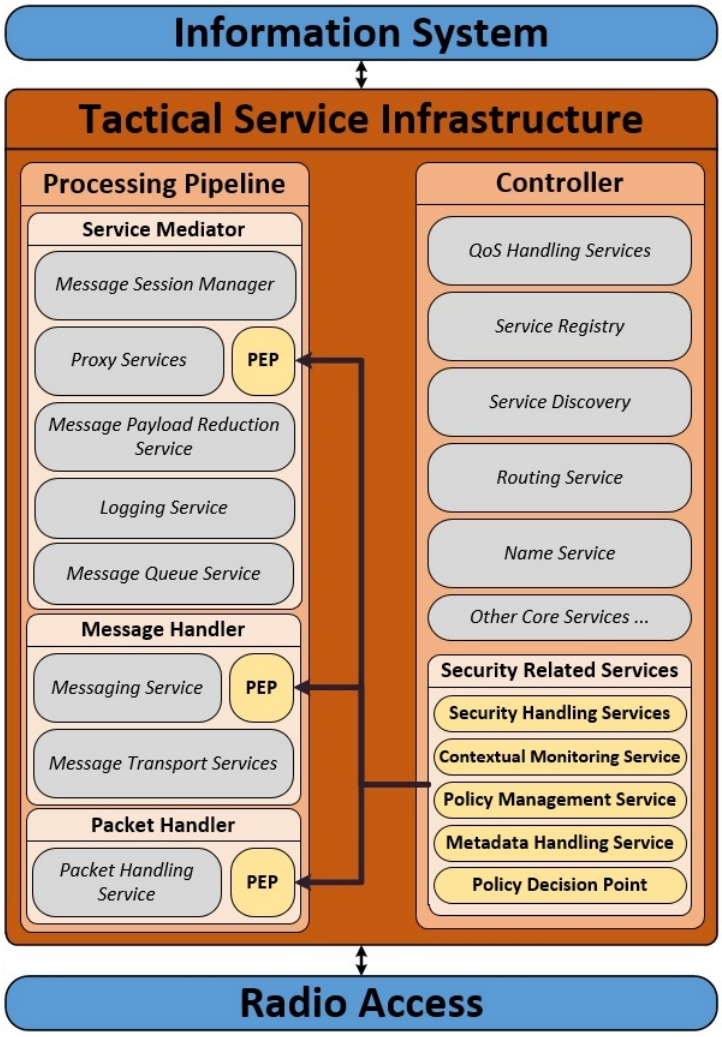

Figure 7.1: Defined internal components of TSI nodes.

1. **Processing Pipeline:** It comprise of the following sub-components:
   - *Service Mediator:* Supports functionalities related to session management, message exchange and message adaptation. The defined functionalities include but are not limited to locate remote services, create proxy services, support various message exchange patterns and adjust message priority.
   - *Message Handler:* Supports functionalities related to message forwarding and message transport. The defined functionalities include but are not limited to message format translation, next hop identification, message monitoring and message storage management.
   - *Packet Handler:* Supports functionalities related to packet forwarding and packet scheduling. The defined functionalities include but are not limited to reliability handling, packet queue handling and packet release to radio.
2. **Controller:** It includes core services responsible for the supervision of the aforementioned services, deployed across the processing pipeline layers. The defined functionalities include but are not limited to trigger resource reservation, update service endpoints, select routing protocol and enforce encryption mechanisms.

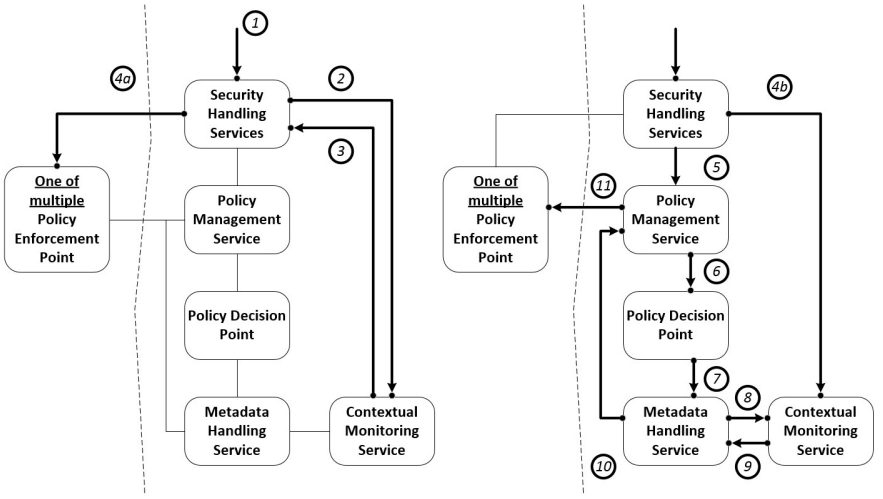

Figure 7.2: Interaction of security services within the TSI.

The aforementioned security services along with the interactions supported by the defined interfaces are presented at figure 7.2. As described earlier in detail [20], the functionalities of these elements can be summarised as:

- **Security Handling Service-(SH):** A service that monitors network parameters and actors behaviour or requests, where actors can be users, nodes and services. Accordingly it identifies the requirement for a specific action, initiating a corresponding action request. Additionally, SH stores precomputed policy decisions, either from the mission preparation stage or by earlier requests during mission execution, for optimization of resource utilization.

- **Policy Management Service-(PM):** A service that is responsible for the successful resolution of the action request in accordance to the current network parameters and its subsequent transfer for enforcement.

- **Policy Decision Point-(PDP):** It contains the policy rules mapped to the available action requests, in the form of prioritised description logic queries.

- **Metadata Handling Service-(MH):** An ontological knowledge-base, which incorporates static and dynamic attributes required for reasoning over the aforementioned policy rules. Reasoning occurs at the MH in accordance to a static copy of the ontological structure at the time of the action request in order to maintain policy consistency.

- **Contextual Monitoring Service-(CM):** A service that monitors timely values of the dynamic attributes utilised across the policy rules, while it computes statistical and aggregated values populating MH upon request.

- **Policy Enforcement Point-(PEP):** A service responsible for the enforcement of the generated or precomputed policy decisions, by use of the locally implemented mechanisms.

While in respect to the functionalities of the implemented interfaces:

- **1:** SH receives a trigger for the initiation of an action request. The trigger can be either external (e.g. access request by a user, service invocation request by a service, message prioritization request by Quality of Service (QoS) mechanisms) or internal by monitoring the values of the dynamic attributes stored at CM (e.g. node trust levels, node location updates, service choreography statistics).

- **2:** SH requests from CM the current values of the attributes related to the given action request. These values are compared with a predefined range for which the precomputed policy decisions are valid.
- **3:** CM replies with the timely values of the requested dynamic attributes.
- **4a:** If the received attribute values correspond to the predefined ranges, the precomputed policy decision is transferred to the corresponding PEP for enforcement. In this scenario the procedure is successfully terminated at this stage.
- **4b:** If the received attribute values are outside the predefined ranges, SH sends a request to CM for a static copy of the monitored parameters with a unique identifier.
- **5:** SH sends an action solution request to the PM including the unique identifier.
- **6:** PM sends the same bundle (Action Solution Request, Unique Identifier) to the PDP, which retrieves the stored set of prioritised rules corresponding to the given action request.
- **7:** PDP populates the bundle with the first priority rule (Action Solution Request, Unique Identifier, 1st Priority Rule) and transfers it to the MH.
- **8:** MH requests the values of the monitored parameters corresponding to the received Unique Identifier.
- **9:** MH receives the aforementioned values and populates a locally stored copy of the ontological knowledge-base. At this stage, reasoning occurs using this copy and the received 1st Priority Rule.
- **10:** The identified instances are transferred to PM. (Note: If no instances have been identified, steps 6 to 10 are repeated using the complementary prioritised rules)
- **11:** The policy decision is transferred to the PEP for enforcement.

7.3 Formal Policy Modelling

7.3.1 Core Policy Model

The formal policy model has been constructed by mapping the aforementioned architectural elements to the required functionalities, as presented at figure 7.3. The decision process within the formal policy model is:

Equation 7.1:
$Individual\_Domain \cap Individual\_Capability = \{Individual\_Action(k), Individual\_Action(k+1), ..., Individual\_Action(k+i)\}$

Where:

Equation 7.2:
$Individual\_Action(k) \widehat{=} \{Individual\_Rule[k(z)], Individual\_Rule[k(z+1)], ..., Individual\_Rule[k(z+j)]\}$

And:

Equation 7.3:
$$Observable\_Objects \xrightarrow{Indivi.\_Rulek(z)} Governing\_Mechanisms_{Individual\_Action(k)}$$

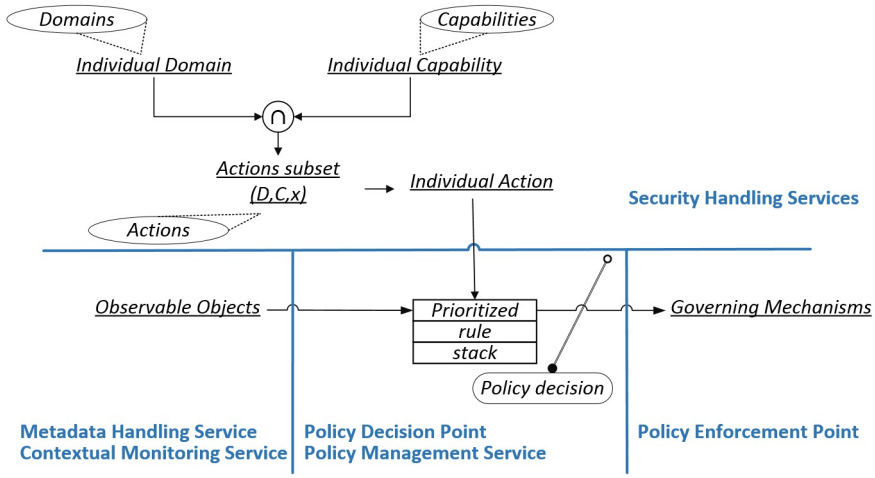

Figure 7.3: Visualisation of the decision process within the formal policy model.

While the elements constituting the formal policy model have been defined as:

- **Domains:** The tactical policy domains have been identified in accordance to the protection requirements as Planning, Protection, Detection, Diligence and Response. These generic core domains can be extended or refined in order to support fine-grained definition of policy governance.

Individual Domain: A singular Domain corresponding to the evaluated action.

- **Capabilities:** TACTICS defined a distinct set of capabilities as part of the developed TRA, in accordance to contemporary operational requirements and the existing NATO Capability View (NAF-NCV-2/ 7 [14]). The extended list of defined capabilities includes Effects Management, Fire Support, Combat Service Support and Shared Situational Awareness.

  Individual Capability: A singular Capability corresponding to the evaluated action.

- **Actions:** Actions are defined as the intersection of Domains and Capabilities, in the sense of enforcing the Domain requirements upon the operational Capabilities. Thus, defining fine grained policy sub-trees such as Planning/ Effect Management, Protection/ Shared Situational Awareness or Response/ Intrusion Detection.

  Actions subset: A subset of available, suitable and prioritised responses in respect to the defined Actions, by the activation and tailored management of the available Governing Mechanisms. In that sense the Action "Protection/ Message Transmission", may correspond to an Action subset that includes various cryptographic and credential management services

  Individual Action: A singular policy response across the examined Action subset.
  Note: The definition of these elements allow the Security Handling Services to identify and initiate fine-grained policy decisions, as mapped in a prioritised order to the monitored Observable Objects and actor behaviour or requests.

- **Observable Objects:** Monitored network parameters of static and dynamic nature, as predefined during the mission preparation stage. Observable Objects refer to Service, Information, Network, Radio, Node and Subject attributes, formulating a complete description of the tactical SOA ecosystem upon which policy reasoning is achieved.
  Note: The Metadata Handling Service maintains a static local knowledge according to the values of Observable Objects in an ontological knowledge base, while the Contextual Monitoring Service is responsible for the monitoring of dynamic Observable Objects and the calculation of their timely, statistical and aggregated values.

- **Prioritized rule stack:** A set of predefined and prioritized rules dedicated to the governance of each Individual Action. Every rule is constructed as a description logic query for instance identification, with

increased granularity as a function of Observable Objects.
Note: The definition of multiple rules for the governance of each Individual Action allows the on-line adaptation of policy decisions to the dynamic network conditions, in contrast to singular implementations. The communication between the Policy Decision Point and Policy Management Service facilitates the selection of the most suitable governing rule at the decision time, according to predefined prioritizations

- **Governing Mechanisms:** Services deployed within the Policy Decision Point capable of enforcing the policy decision in respect to an examined Individual Action.
  Note: The deployed Governing Mechanisms can be generic or mission specific, related to a variety of security requirements such as authentication, authorisation, cryptography, session management, access control, integrity control, error handling/logging, validation and public key infrastructure.

7.3.2 Policy Formalization

The formalisation of the core policy model elements within the security TSI services, is based on suitable description logic fragments and executed in six consecutive steps. These steps are in direct mapping to the decision process, as presented in Equations 7.1, 7.2, and 7.3. Various detailed resources exist in respect to knowledge representation with description logic [2]. Thus, the purpose of this subsection is not to provide an exhaustive reference to this topic, but an insight to the elements crucial for the formalization of the developed security policy model:

- **Equation 7.1**

  Step 1-Definition of Domains:
  Individual Domains are initially formalised as empty disjoint ontology classes, using terminological box concept definitions. These classes are consequently populated with the defined Actions, formalising extensional knowledge in the form of simple membership assertions, as:

  Equation 7.4:
  $hasDomain(AccessDenial, Response)$

  A closed world assumption must be enforced in order to accommodate the functionality of the Security Handling Services in respect to Action identification. This is achieved in ontology editors by the definition of restricted equivalences for each domain class using a functional data property (e.g. hasDomain). As an example in OWL functional syntax,

this is defined as:

```
Declaration(Class(:Domains))
Declaration(Class(:Response))
SubClassOf(:Response :Domains)
EquivalentClasses(:Response DataHasValue(:hasDomain "
    ↪ Response"))
Declaration(DataProperty(:hasDomain))
FunctionalDataProperty(:hasDomain)
DataPropertyRange(:hasDomain DataOneOf("Defined Domains")
    ↪ )
Declaration(NamedIndividual(:AccessDenial))
DataPropertyAssertion(:hasDomain :AccessDenial "Response"
    ↪ xsd:string)
```

Step 2-Definition of Capabilities:
Capabilities are formalised and populated similarly to Domains, as:

```
Declaration(Class(:Capabilities))
Declaration(Class(:MessageAuthenticityAssurance))
SubClassOf(:MessageAuthenticityAssurance :Capabilities)
EquivalentClasses(:MessageAuthenticityAssurance
    ↪ DataHasValue(:hasCapability "
    ↪ MessageAuthenticityAssurance"))
Declaration(DataProperty(:hasCapability))
FunctionalDataProperty(:hasCapability)
DataPropertyRange(:hasCapability DataOneOf("Defined
    ↪ Capabilities"))
Declaration(NamedIndividual(:DigitalSignatureValidation))
DataPropertyAssertion(:hasCapability:
    ↪ DigitalSignatureValidation "
    ↪ MessageAuthenticityAssurance"xsd:string)
```

Step 3-Definition of Actions and Grouping into Actions subsets:
Actions are formalised as individuals with the use of unary predicates and categorised into Action subsets with the use of existential quantifications and value restrictions. This is achieved in ontology editors with the definition of data properties of suitable granularity. As mentioned earlier, the Security Handling Service initiates an Action based policy request in accordance to external or internal triggers. An external trigger is directed to a singular Action (e.g. Domain: Protection/ Capability: ServiceAccessControl/ Action: AccessMessagingService), while an internal trigger is based on the dynamic values of predefined Observable Objects leading to the identification and evaluation of multiple actions defined as an Action subset. Thus the Actions forming

each Action subset must be prioritised in order to accommodate this functionality, allowing the identification and enforcement of the most suitable policy decision in accordance to the existing resources. Description logic allows the fine-grained definition of Actions. In the previous simplified example, the Action definition is represented in OWL functional syntax as:

```
Declaration(DataProperty(:hasActionSetID))
Declaration(DataProperty(:hasActionSetPriority))
Declaration(DataProperty(:hasCapability))
Declaration(DataProperty(:hasDomain))
Declaration(DataProperty(:hasGoverningMechanism))
Declaration(DataProperty(:hasRuleSetID))
Declaration(NamedIndividual(:AccessMessagingService))
FunctionalDataProperty(:hasActionSetID)
DataPropertyRange(:hasActionSetID xsd:integer)
FunctionalDataProperty(:hasActionSetPriority)
DataPropertyRange(:hasActionSetPriority xsd:integer)
FunctionalDataProperty(:hasCapability)
DataPropertyRange(:hasCapability DataOneOf("Defined
    ↪ Capabilities"))
FunctionalDataProperty(:hasDomain)
DataPropertyRange(:hasDomain DataOneOf("Defined Domains})
    ↪ )
DataPropertyRange(:hasGoverningMechanism xsd:string)
FunctionalDataProperty(:hasRuleSetID)
DataPropertyRange(:hasRuleSetID xsd:integer)
DataPropertyAssertion(:hasActionSetID :
    ↪ AccessMessagingService "9632654"xsd:integer)
DataPropertyAssertion(:hasActionSetPriority :
    ↪ AccessMessagingService "1" xsd:integer)
DataPropertyAssertion(:hasCapability :
    ↪ AccessMessagingService "ServiceAccessControl" xsd:
    ↪ string)
DataPropertyAssertion(:hasDomain :AccessMessagingService
    ↪ "Protection" xsd:string)
DataPropertyAssertion(:hasGoverningMechanism :
    ↪ AccessMessagingService "AuthServ23" xsd:string)
DataPropertyAssertion(:hasRuleSetID :
    ↪ AccessMessagingService
"86514665" xsd:integer)
```

It must be noted that in terms of ease of implementation and deployment, the same procedure can be used for the definition of Action clusters according to invocation and statistical patterns. Utilising constrained class equivalences and exceptions, Actions of separate Action

subsets can be efficiently grouped and mapped into common policy rules, significantly minimising resource consumption under heavily constrained scenarios.

- **Equation 7.2**

  Step 4-Definition of Prioritised rule stack per Action:
  The notable expressive power of description logic fragments originates from the extended set of available constructors, including but not limited to elements of first order logic (e.g intersection, union, complement, universal/ existential restriction) and role oriented (e.g. role union/ chains/ transitivity/ hierarchy). The full extend of available constructors can be exploited at this step for the definition of detailed rules of increased granularity, incorporating both unary and binary predicates in accordance to the security requirements.

  Thus, a prioritized rule stack of increasing complexity is defined per Action, facilitating the adaptation of the security policy to dynamic network conditions. The least-priority/ least-complexity rule for each Action is defined as a default escape policy expression (i.e. deny-override, permit-override, deny-by-default, permit-by-default) depending on the type of the Action, for use in highly congested tactical environments and node isolation scenarios. Concurrently, the rules of highest priority can designedly incorporate sets of unary and binary predicates, referring to discrete adaptations of the security policy to the real time network conditions for the given Action.

- **Equation 7.3**

  Step 5-Extraction of Observable Objects and knowledge base construction:

  Observable Objects correspond to the aforementioned unary and binary predicates referring to service, information, network, radio, node and subject attributes as incorporated within the policy rules. Observable Objects can be defined in ontology editors as object and data properties, enforcing suitable schema constructs (e.g. subPropertyOf, range), relations to other properties (e.g. inverseOf), logical characteristics (e.g. transitive, symmetric) and global cardinality restrictions (e.g. InverseFunctionalProperty, FunctionalProperty). Depending on the granularity requirements of the defined policy rules aggregated and statistical Observable Objects can also be constructed and incorporated, allowing their utilisation across rules of distinct priority levels.

  Step 6-Mapping of Individual Actions to Governing Mechanisms:
  This step is initiated during Step-3 by the definition of suitable DataPropertyAssertions, and finalised by a constrained mapping between

actions and suitable Governing Mechanisms for their enforcement. This is achieved by the definition of simple membership assertions, similar to those presented in previous steps.

7.4 Prototype Implementation

TACTICS has defined sixty requirements with "MUST" priority, forty with "SHOULD" and seven with "COULD", thirty-four of which are security dedicated as briefly discussed earlier [1][9]. An overall prototype implementation has been realised according to sections 7.2 and 7.3, in order to validate the satisfaction of these requirements under the distinct tactical constraints. This implementation was targeted to four common tactical operation types (1-Reconnaissance Surveillance and Target Acquisition, 2-MEDical EVACuation, 3-Convoy mission, 4-Intervention Patrol), separated into a multitude of corresponding episodes (e.g. Sensor data acquisition, Blue force tracking, Mobility management, Improvised Explosive Device detection and report, Ordering and Tasking). Here we present the security policy formalization, in respect to the interface functionalities as presented at sections 7.2 and 7.3, for one of the investigated episodes.

7.4.1 Transitive service invocation

The presented example is part of the transitive service invocation scenarios of the convoy mission use case. Nodes N1 and N2 are mounted on vehicles that belong to a tactical convoy, with N1 being the command vehicle and N3 a hand-held device (TSI Node Dismounted) allocated to a member of N2 personnel. The scenes of the episode are:

1. N1 requires an image from the Area of Operation(AoO) of N2.
2. N1 Identifies available services*.
3. N1 Identifies local service provider*.
4. N1 Transmits corresponding request to N2.
5. N2 Transmits corresponding request to N3.
6. N3 Evaluates service access request* .
7. N3 Invokes service.
8. N3 Identifies image compression requirement*.
9. N3 Identifies local service provider*.
10. N3 Transmits uncompressed image to N2.

11. N2 Evaluates service access request * (according to image attributes and N3 credentials).

12. N2 Invokes service.

13. N2 Transmits compressed image to N1.

The overall execution of a transitive service invocation corresponds to a variety of Actions including interactions between the Information System, TSI, and Radio Access, with load both on the northbound/ southbound interfaces and core service invocations within and across the involved tactical nodes. For clarity these functionalities have been distributed across multiple use cases, while those corresponding to this scenario are marked as "*". Although multiple security policy decisions are involved within a transitive service invocation, this scenario is one of those dedicated to investigating specific aspects of the service choreography functionalities. Thus, actions related to message transmission and queuing, bandwidth allocation or service substitution refer to the invocation of a variety of TSI core services [6], which are not within the scope of this scenario.

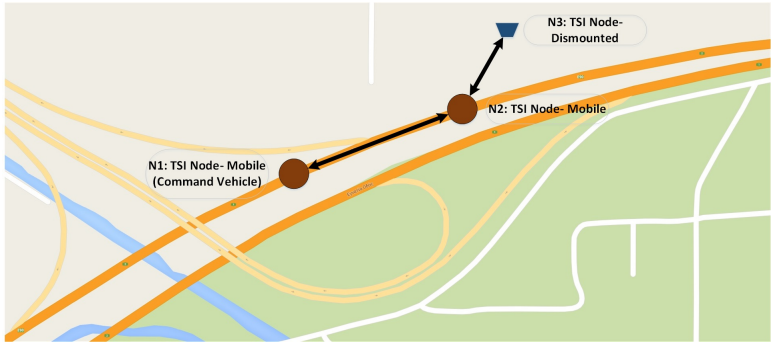

Figure 7.4: Visualisation of transitive service invocation scenario.

The policy formalisation in OWL functional syntax for the presented steps 1-6, can be extracted for this episode as:

- *Step 1-Definition of Domain:*
  Only the Protection Domain is required within the given scenario, defined as presented at subsection 7.3.2.

- *Step 2-Definition of Capabilities:*
  The given scenario refers to the Service_Choreography and Situational _Awareness capabilities, defined as presented at subsection 7.3.2.

- *Step 3-Definition of Actions and Grouping into Actions subsets:*
  The presented functionalities correspond to four of the Actions within the Action subsets defined by the Protection/ Service_Choreography and Protection/ Situational_Awareness intersections, namely:

  1. Service_ServiceAvailabilityIdentification.
  2. Node_LocalServiceProviderIdentification.
  3. Service_ServiceAccessRequestVerification.
  4. Information_ImageAttributeIdentification.

  which are defined as presented at subsection 7.3.2.

- *Step 4-Definition of Prioritised rule stack per action:*
  As described earlier, making use of the extended expressive power of description logic allows the construction of complex security policy rules, validating unary and binary predicates as needed by the specific Action. Using as a simplified example the Node_LocalServiceProvider Identification Action the Prioritised rule stack in Manchester syntax can have the form:

  1. 1st priority rule:

```
Node_SupportsService value "TacticsImaging"
Node_hasUser some AllSubjects
(User_hasTrustLevel value "High") and  ((
    ↪ Node_hasTrustLevel value "High") or (
    ↪ Node_hasTrustLevel value "Medium"))
Node_hasAoO value "AoO12341"
(User_hasRank value "COL") or (User_hasRank value "
    ↪ CPT")
Node_hasMissionType value "Convoy"
(Node_hasOperationalGroup value "G2") and (
    ↪ Node_hasType value "TSI_ND")
Node_hasSupportRadioITUDesignation value "UHF"
Node_hasSupportProtocol value "TLS/SSH"
```

  2. 2nd priority rule:

```
Node_SupportsService value "TacticsImaging"
Node_hasUser some AllSubjects
(User_hasTrustLevel value "High") and ((
    ↪ Node_hasTrustLevel value "High") or (
    ↪ Node_hasTrustLevel value "Medium"))
Node_hasAoO value "AoO12341"
Node_hasOperationalGroup value "G2"
```

```
Node_hasSupportRadioITUDesignation value "UHF"
Node_hasSupportProtocol value "TLS/SSH"
```

3. 3rd priority rule:

```
Node_SupportsService value "TacticsImaging"
Node_hasUser some AllSubjects
(User_hasTrustLevel value "High") and ((
    ↪ Node_hasTrustLevel value "High") or (
    ↪ Node_hasTrustLevel value "Medium"))
Node_hasAoO value "AoO12341"
Node_hasSupportProtocol value "TLS/SSH"
```

4. 4th priority rule:

```
Node_SupportsService value "TacticsImaging"
```

- *Step 5-Extraction of Observable Objects and knowledge base construction:* Using the previous rule set as an example the Observable Objects can be extracted as:

  1. **Data properties (Unary predicates):**
     User_hasTrustLevel,
     Node_hasTrustLevel,
     Node_hasAoO,
     User_hasRank,
     Node_hasMissionType,
     Node_hasOperationalGroup,
     Node_hasType,
     Node_hasSupportProtocol
  2. **Object properties (Binary predicates):**
     Node_SupportsService,
     Node_hasUser,
     Node_hasSupportRadioITUDesignation

  The overall extracted Observable Objects incorporated within the security policy knowledge-base are defined as presented at subsection 7.3.2 and described earlier [9].

- *Step 6-Mapping of individual Actions to Governing Mechanisms:* This step depends on the locally implemented services across the nodes deployed for a given tactical operation. Thus, as an example in the given scenario, the Service_ServiceAvailabilityIdentification Action would have as first priority Governing Mechanism the distributed

service registry, while the security policy knowledge-base could also serve as a secondary Governing Mechanism for redundancy purposes.

7.5 Conclusions

In this article we have presented a security policy framework dedicated to tactical SOA, aiming to satisfy the established protection requirements under the constraints of tactical environments. The developed architecture has been presented, focusing on the functionalities of core services and an insight of the defined interfaces. Furthermore, the formal policy model was presented along with the required policy formalisation steps. The prototype implementation has provided a validation of the requirement for an easily deployed, lightweight, cross-layer and dynamically adaptable security infrastructure. Thus, our future plans include the further evaluation with the use of the developed use cases and the preparation of the field-demonstration along with the overall TACTICS architecture.

Acknowledgments

The results described in this work were obtained as part of the European Defence Agency project TACTICS (Tactical Service Oriented Architecture). The TACTICS project is jointly undertaken by Patria (FI), Thales Communications & Security (FR), Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE (DE), Thales Deutschland (DE), Leonardo (IT), Thales Italia (IT), Norwegian University of Science and Technology (NO), ITTI (PL), Military Communication Institute (PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980.

Bibliography

[1] ALOISIO, A., AUTILI, M., D'ANGELO, A., VIIDANOJA, A., LEGUAY, J., GINZLER, T., LAMPE, T., SPAGNOLO, L., WOLTHUSEN, S. D., FLIZIKOWSKI, A., AND SLIWA, J. TACTICS: TACTICal Service Oriented Architecture. *CoRR abs/1504.07578* (2015). Available from: `http://arxiv.org/abs/1504.07578`. 43, 63, 103, 121, 143, 154, 189, 191, 212

[2] BAADER, F., CALVANESE, D., MCGUINNESS, D. L., NARDI, D., AND PATEL-SCHNEIDER, P. F., Eds. *The Description Logic Handbook: Theory, Implementation, and Applications*. Cambridge University Press, New York, NY, USA, 2003. 150

[3] BECKER, M., AND SEWELL, P. Cassandra: distributed access control policies with tunable expressiveness. In *Policies for Distributed Systems and Networks, 2004. POLICY 2004. Proceedings. Fifth IEEE International Workshop on* (June 2004), pp. 159–168. 84, 143, 165

[4] CZENKO, M., DOUMEN, J., AND ETALLE, S. Trust management in p2p systems using standard tulip. In *Trust Management II*, Y. Karabulut, J. Mitchell, P. Herrmann, and C. Jensen, Eds., vol. 263 of *IFIP The International Federation for Information Processing*. Springer US, 2008, pp. 1–16. Available from: `http://dx.doi.org/10.1007/978-0-387-09428-1_1`. 84, 143, 165

[5] DAMIANOU, N., DULAY, N., LUPU, E., AND SLOMAN, M. The ponder policy specification language. *Policy 1* (2001), 18–38. 18, 19, 84, 143, 165, 215

[6] DIEFENBACH, A., GINZLER, T., MCLAUGHLIN, S., SLIWA, J., LAMPE, T. A., AND PRASSE, C. Tactics tsi architecture: A european reference architecture for tactical soa. In *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (May 2016), pp. 1–8. 63, 103, 121, 144, 155, 218

[7] FININ, T., JOSHI, A., KAGAL, L., NIU, J., SANDHU, R., WINSBOROUGH, W. H., AND THURAISINGHAM, B. ROWLBAC - Representing

Role Based Access Control in OWL. In *Proceedings of the 13th Symposium on Access control Models and Technologies* (Estes Park, Colorado, USA, June 2008), ACM Press. 84, 143, 165, 189

[8] GKIOULOS, V., AND WOLTHUSEN, S. D. Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks. *Norwegian Information Security Conference - NISK* (2015), 109–120. 43, 63, 103, 113, 122, 123, 143, 166, 168, 189, 191, 213, 218, 220

[9] GKIOULOS, V., AND WOLTHUSEN, S. D. Securing tactical service oriented architectures. In *2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)* (July 2016), pp. 1–6. 63, 71, 103, 113, 122, 123, 143, 154, 157, 189, 191, 213, 218, 220

[10] GKIOULOS, V., AND WOLTHUSEN, S. D. *Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures*. Springer International Publishing, Cham, 2017, pp. 149–166. Available from: http://dx.doi.org/10.1007/978-3-319-44354-6_9. 43, 63, 103, 113, 114, 122, 123, 143, 189, 191, 213, 218, 223

[11] KAGAL, L., FININ, T., PAOLUCCI, M., SRINIVASAN, N., SYCARA, K., AND DENKER, G. Authorization and privacy for semantic web services. *Intelligent Systems, IEEE 19*, 4 (Jul 2004), 50–56. 84, 143, 165

[12] KOLTER, J., SCHILLINGER, R., AND PERNUL, G. Building a distributed semantic-aware security architecture. In *New Approaches for Security, Privacy and Trust in Complex Environments*, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, Eds., vol. 232 of *IFIP International Federation for Information Processing*. Springer US, 2007, pp. 397–408. Available from: http://dx.doi.org/10.1007/978-0-387-72367-9_34. 84, 143, 165

[13] LI, N., MITCHELL, J., AND WINSBOROUGH, W. Design of a role-based trust-management framework. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on* (2002), pp. 114–130. 84, 143, 165

[14] NATO. Nato c3 classification taxonomy. https://www.act.nato.int/article-8a, 2012 March. 84, 149

[15] NEJDL, W., OLMEDILLA, D., AND WINSLETT, M. Peertrust: Automated trust negotiation for peers on the semantic web. In *Secure Data Management*, W. Jonker and M. Petkovi, Eds., vol. 3178 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2004, pp. 118–132. Available from: http://dx.doi.org/10.1007/978-3-540-30073-1_9. 84, 143, 165

[16] OASIS. OASIS Security Services (SAML) TC. Available from: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security. 84, 143, 165, 214

[17] RAMLI, C. D. P. K., NIELSON, H. R., AND NIELSON, F. The Logic of XACML. *Science of Computer Programming 83* (Apr. 2014), 80–105. 84, 143, 165, 214

[18] TRIVELLATO, D., ZANNONE, N., GLAUNDRUP, M., SKOWRONEK, J., AND ETALLE, S. A semantic security framework for systems of systems. *International journal of cooperative information systems 22*, 01 (2013), 1350004. 20, 84, 143, 165, 189, 190, 215

[19] USZOK, A., BRADSHAW, J., JEFFERS, R., SURI, N., HAYES, P., BREEDY, M., BUNCH, L., JOHNSON, M., KULKARNI, S., AND LOTT, J. Kaos policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement. In *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks* (June 2003), pp. 93–96. 143, 165, 215

[20] VASILEIOS, G., WOLTHUSEN, S. D., FLIZIKOWSKI, A., STACHOWICZ, A., NOGALSKI, D., GLEBA, K., AND SLIWA, J. Interoperability of security and quality of service policies over tactical SOA. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)* (Dec 2016), pp. 1–7. 63, 103, 146, 214, 227

Chapter 8

Article 3b: Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures

Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures

Advances in Network Systems, Advances in Intelligent Systems and Computing, Springer, AISC, volume 461, pp. 149-166.

Gkioulos, Vasileios Wolthusen, Stephen D.

Abstract

Tactical networks are typically of an ad-hoc nature operating in highly restricted environments and under constrained resources. The frequent presence of communication disruptions and network partitioning must also be expected and managed, while core functionalities must be maintained, providing asynchronous invocation and access to services in a distributed manner. Supporting the required functionalities of the contemporary tactical environment, requires the dynamic evaluation of security policies, incorporating semantic knowledge from various network layers, together with facts and rules that are defined axiomatically a priori. However, the required basis for such policy decisions can be excessively extended and dynamic. Thus, it is desirable to locally minimize the scope of the policy maximizing efficiency. In this paper, we therefore analyze criteria and optimization goals for the a priori distribution and partitioning of security policies, ensuring the continuous support of the required capabilities, given the operational tasks of each deployed actor.

8.1 Introduction

Tactical networks refer to mobile networks, with characteristics similar to Ad-Hoc and mesh structures. They are typically adjusted and deployed to serve the specifics of a particular operation, with characteristics known partially in advance. Consequently, the study, evaluation and realization of globally suitable security mechanisms, must be able to dynamically adapt to the versatile and diverse nature of tactical operations. The tactical environment is continuously studied, both in terms of operational analysis and

technical evaluation [23, 5, 10, 14, 44], allowing the extraction of valuable information regarding their nature, characteristics and requirements.

The deployed assets for a specific operation should be expected to operate over distinct platforms, with diverse capabilities and requirements, including the ability to operate in coalition environments. Additionally, due to resource limitations and the dynamically evolving topologies, no safe assumptions can be made regarding continuous connectivity, since a tactical network may degrade to the point of partitioning. For the same reasons, communication failures, uncertain service delivery and extensive delays must be expected and properly addressed. Within this environment, tactical networks must be able to provide reliable and secure service delivery and communication. Hence, the realized security mechanisms have to be distributed across the deployed assets, since no centralized security dedicated entity can be assumed, due to inability of reassuring a continuously available link towards it.

In addition to the aforementioned constraints, the introduction and increasing requirement of supporting NEC and NCW, formulated a new set of requisite features regarding the functionalities of contemporary tactical networks [35, 2, 46]. Thus, mechanisms based on the SOA paradigm emerged as the most suitable mediators for the realization of these requirements, within the deployed C4I and C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) systems. [31, 26, 48, 24, 25, 33, 34].

Securing tactical SOA requires not only the accomplishment of general information protection goals (such as confidentiality, availability, authenticity and control) but also the dynamic protection of communication, data at rest and processing, within the aforementioned restrictions imposed by their nature. The realization of suitable security mechanisms requires the conceptualization of the multitudinous semantic attributes available across the network. Such elements rise among others from services, terminals, information, communication links and subjects, alongside their relations and interactions.

Well known mechanisms (such as WS-Security, Ponder [13], SAML [39], XACML [43], RT [30], Cassandra [6], Peer-Trust [37], Tulip [12], ROWLBAC [16], REI[27], KAOS [50], Kolter et al. [29]) have been extensively studied and found to be unsuitable for the contemporary tactical environment for a variety of reasons. Some face limitations in capturing and expressing the required semantics, others are relatively heavyweight regarding their computational and communication requirements, or lack the ability of decentralized operation. Furthermore, some are not rigorous and flexible enough in expressing and reasoning over security policies, face scalability limitations or a combination of these reasons. These studies (including but not limited to [15, 7, 22, 8, 47, 38, 16, 28, 49]) promoted the use of ontologies for

the definition of general purpose security policies, due to their expressive power and ability to overcome the aforementioned constraints.

For the same reasons in our previous study [20] we proposed a framework for the realization of an ontologically defined security infrastructure, with the use of OWL, suitably adjusted to the constraints and high level functional requirements of tactical SOA. Yet, although ontologies can provide the required extended scope over the existing semantic attributes, the aforementioned inability to rely on a centralized security dedicated entity requires the distribution of the defined mechanisms across the deployed tactical nodes. However, due the functional limitations of tactical nodes (e.g. computational capacity, storage capacity, bandwidth availability), mere replication of those mechanisms across the network is inefficient and commonly infeasible.

In this paper we present our findings regarding the partitioning and distribution of ontologically defined security policies, suitably adjusted to the specifics of tactical SOA, aiming to maximize efficiency by minimizing the local scope of the policy. We approach this topic by identifying the criteria rising from the nature of tactical SOA, seeking a reliable limitation to a problem similar in nature to a 0-1 multiple knapsack problem, therefore subject to existing mechanisms of discrete optimization. Furthermore, we identify suitable elements in order to minimize the complexity by reducing the number of instances, maintaining the complete set of functionalities supported by the defined security policies.

8.2 Ontologically Defined Security Policies for Tactical SOA

An ontologically defined security policy dedicated to the specifics of tactical SOA must be able to provide the dynamic protection of communication, data at rest and processing, alongside the general information protection goals. Such a mechanism requires the conceptualization of the assorted semantic attributes, within a robust yet flexible mapping between the involved elements. These elements comprise of the defined *Domains* (including but not limited to planning, protection, diligence, detection and response), the required *Capabilities* (similar to NATO Architecture Framework/ NATO Capability View (NAF/ NCV) [1], including but not limited to core, application, communication and inter-domain), the available *Actions* and a set of governing *Rules* for each action, each of which incorporates a varying set of the involved *Conditions* (which correspond to the aforementioned dynamic and static semantics). An outline of the security policy structure, including the overlaying relations, is presented at figure 8.1.

These elements are defined as OWL classes, which are populated according to the requirements of each tactical operation. The Security_Core is the

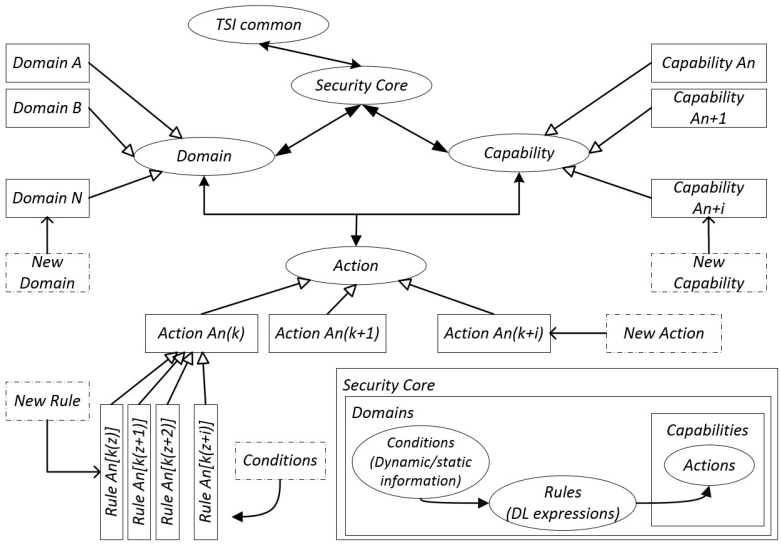

Figure 8.1: Outline of security policy structure

anchor of the policy structure similar to owl:Thing of ontologies, incorporating all the other elements as subclasses. Furthermore, the Security_Core is the gateway towards the TSI_common (Tactical Service Infrastructure common core ontologies) and additional ontologies that are required to be linked with the security infrastructure. Thus, through the Security_Core the security policy can monitor the functionality of the enabled capabilities, within each tactical domain. This is achieved by the on-line evaluation of the environmental conditions, through the set of governing rules established for each action.

This framework permits the multi-domain and cross-layer implementation of security policies. Making use of the expressive power of description logic, complex relations can be established between the defined elements. Thus, actions within a specific capability can be linked to trigger the conditions evaluation of a rule established over a different domain. Additionally, conditions collected from various layers can affect decisions on other layers. Namely, a condition within the physical layer can affect a decision regarding the application layer.

The conceptualization of the policy framework is achieved by the use of unary and binary predicates, which are utilised to define the various network entities (data, services, users, terminals) and the relationships among them. Thus, a complete representation of the network can be achieved by defining the distinct constituting elements and their relations, as part of the tactical terminology. The tactical terminology is constructed within the T-

Box with unique and acyclic concept definition, while the A-Box is used for instance identification with the use of concept and role assertions. A detailed procedure for the ontological definition of security policies dedicated to tactical SOA was described earlier [20].

8.3 Constraint Analysis for the Distribution of Security Policies

Limiting the local scope of the security mechanisms in each tactical node, requires the identification of the parameters enabling the partitioning and distribution of security policies, within the context of tactical SOA. In the following sections, we present our findings regarding the identified parameters of critical impact, as they are presented in table 8.1.

Our study over the functional characteristics of tactical SOA and the operation of ontologically defined security policies, promoted three main categories of governing parameters, regarding the attainment of the required horizontal and vertical security policy distribution. The first category refers to the evaluation of the policy, constructed based on the framework described in figure 8.1, regarding its overall and local complexity. The second category refers to the evaluation and categorization of the deployed tactical nodes, based on their expected functional and operational specialization, alongside their presumably known operating features. The last category refers to the sufficient integration of dynamism, emerging from the aforementioned characteristics of the tactical environment.

Security policy distribution		
Ontology	**Tactical Nodes**	**Dynamism**
1- Syntactic complexity	3- Operational specialization	6- Dynamic attributes
2- Structural complexity	4- Functional specialization	7- Dynamic policy evaluation
	5- Operating features	8- Tactical decision cycle

Table 8.1: Governing parameters for the distribution of security policies

8.3.1 Complexity Inducing Components of Tactical Ontological Constructs

As highlighted earlier, the definition of the ontological security policy is unique for each tactical operation, constructed over an overlaying common framework (figure 8.1).

Regarding the syntactic complexity, OWL is provided in three increasingly expressive subsets that can be used for the definition of suitable security policies, namely OWL-Lite (Exp-time complete complexity), OWL-DL (NExp-time complete complexity) and OWL-Full (Undecidability). OWL-Lite supports simple constraint features and basic classification hierarchies. OWL-DL supports increased expressiveness, maintaining guaranteed computational completeness. Finally, OWL-Full provides maximum expressiveness and syntactic capabilities similar to RDF, yet reasoning is not reassured. A summary of the available constructs within OWL-Lite and OWL-DL is presented in table 8.2. [53, 41, 36]. Furthermore, OWL 2 provides a wide set of subset profiles, supporting assorted accommodation between expressive power and reasoning efficiency. For instance, OWL 2 QL (NLogSpace complete complexity) is dedicated to efficiently supporting extensive instance data and database queries, OWL 2 RL (NP-time complete complexity) is optimized for scalable reasoning without fully utilizing the available expressive power, while OWL 2 EL (P-Time complete complexity) is suitable for large scale definition of properties and classes.

OWL-Lite	
Category	**Constructs**
Constructors	Class, subClassOf, Property, subPropertyOf, domain, Individual.
Restrictions	Restriction, allValuesFrom, someValuesFrom, intersectionOf.
Equality	equivalentClass, equivalentProperty, sameAs, differentFrom.
Cardinality (0 or 1)	minCardinality, maxCardinality
Properties	ObjectProperty, inverseOf, Datatype, Transitive, Symmetric, Functional, InverseFunctional.
OWL-DL (In addition to the aforementioned)	
Values	hasValue
Cardinality (No limitation)	minCardinality, maxCardinality
Class axioms	disjointWith, equivalentClass, complementOf, subClassOf, unionOf, intersectionOf.

Table 8.2: Summary of available constructs within OWL-Lite and OWL-DL

Regarding the structural complexity of the defined security policy, a variety of metrics with significant impact have been identified through our study. Their additive complexity overhead must be contemplated during the initial construction of the security policy, while they can be classified as:

1. **Vocabulary size:** The amount of the defined classes, individuals and properties.
2. **Impurity:** The deviation of the ontological structure from a pure tree form, as a result of the defined rdfs:subClassOf axioms.
3. **Mean inheritance:** The mean overall distance between the defined ancestor classes to the corresponding root classes.
4. **Connectivity:** A measurement of the connection density within the security policy, defined as the average number of connections for each of the defined elements (classes and individuals).

Additionally, estimating the significance of individual classes over the overall functionality of the security policy, is pivotal for the identification of crucial distribution links within the policy structure. Such an estimation is possible with the use of the following metrics, for each of the defined classes.

1. **Direct inheritance:** The number of direct ancestors for each defined class. Meaning the number of subclasses defined based on a specific class and affected by changes within it.
2. **Inheritance exponentiation:** The depth of the most distant ancestor of a given class. It can be used as a measure of information inheritance within classes that belong to the same policy branch.
3. **Individual connectivity:** A connection density measure, referring to a specific class, calculated as the sum of the defined relations from and towards this class.

A representation of how these parameters affect the complexity of the security policy and the time required for reasoning over it, is provided in figure 8.2. In this set from our executed simulations, the Pellet reasoner is used over a basic ontological construct, structured using the ALC(D) fragment, in order to isolate and measure the impact of the value of the Vocabulary_size parameter. Furthermore, figure 8.3 provides an illustration of the global complexity estimation, based on the aforementioned combination of the propagating syntactic and local structural complexities.

8.3.2 Classification and Management of Tactical Nodes

Tactical nodes refer to a plethora of mobile platforms, with restricted operational characteristics and distinct requirements. Achieving a viable security policy distribution, requires the identification and incorporation of their influential attributes, for which we can attain a priori awareness. Our study over the characteristics of tactical nodes and the nature of tactical operations promoted three elements, of significant impact, as presented in table 8.1.

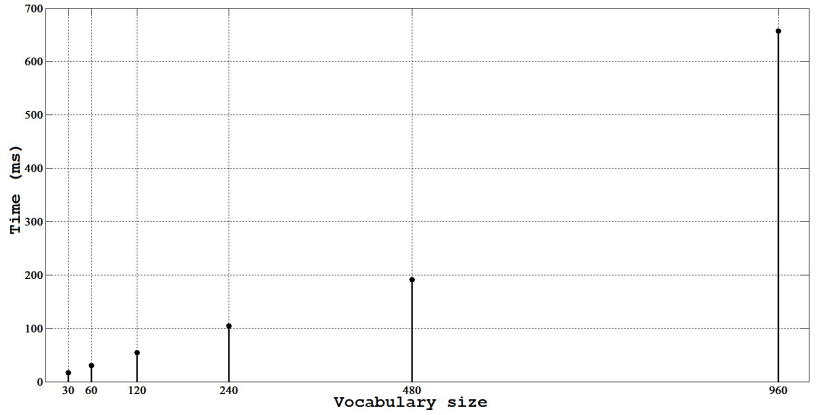

Figure 8.2: Reasoning time escalation in relation to vocabulary size

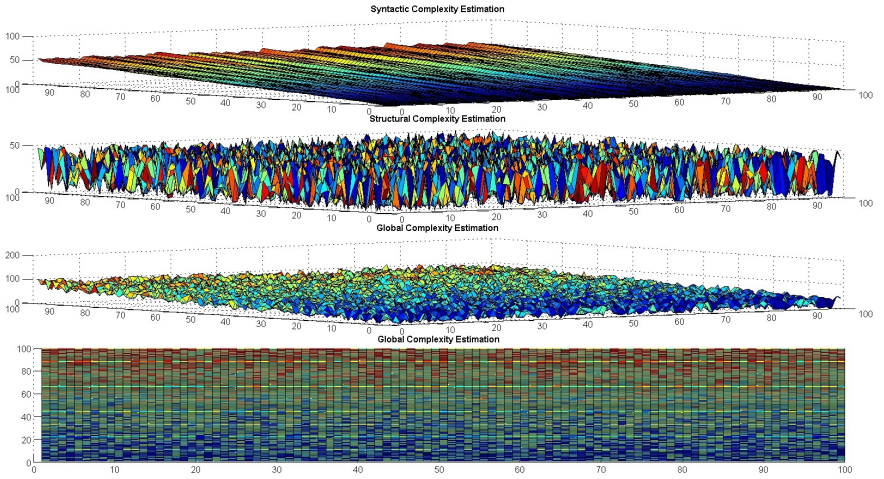

Figure 8.3: Complexity estimation of tactical ontological constructs

The first two elements represent the operational and functional specialization of tactical nodes, rising through the initial operational and contingency planning of a tactical operation. The operational specialization refers to the identification of distinct operational groups among the entirety of the deployed assets, based on their particular strategic objectives. Additionally, functional node specialization, occurs due to the distinct roles of each node within the initial categorization into operational groups (e.g. assuming a tactical team, the hand-held device of a medic, has distinct service/ security requirements from the hand-held device of the team leader or a rifleman).

Hence, the defined operational and functional node specializations can provide an initial classification of nodes, in discrete groups with distinct yet entangled security requirements. This classification can form the basis for the horizontal (in terms of Domain/ Capability groups) or vertical (in terms of Action/ Rule groups), distribution of security policies, incorporating the operational perspective. A representation of the aforementioned procedure is presented in figure 8.4, based on our executed simulations. In this scenario, ten tactical nodes are organised in two operational groups (OG1-square, OG2-circle), while three functional groups (FG1-green(—), FG2-red(|), FG3-blue(\)) are globally defined.

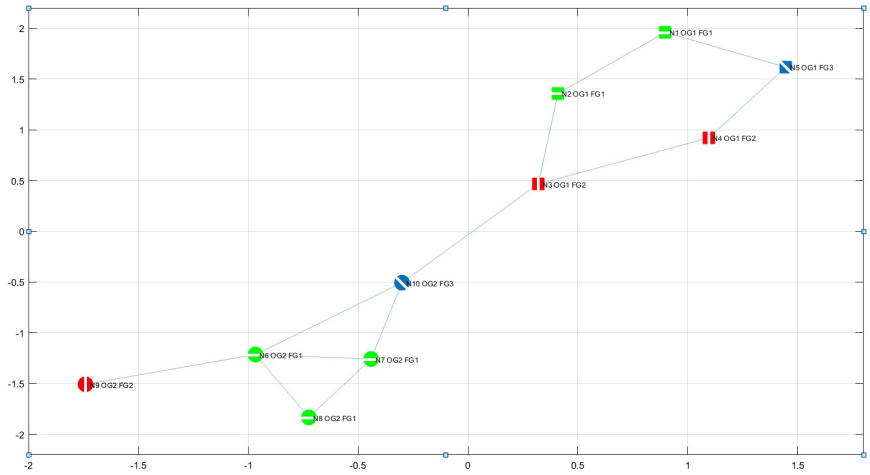

Figure 8.4: Node classification based on operational and functional specialization

An additional element that can significantly affect the distribution of security policies, within tactical SOA, is the presumably known operating features of tactical nodes. Tactical nodes refer to a variety of platforms, which may differ in various terms affecting their performance (grouped afterwards as Computational Capacity). These elements can be classified as:

1. Computational power.
2. Environmental limitations.
3. Physical limitations.
4. Resolution/ accuracy limitations.
5. Input/ output limitations.

6. Range/ coverage limitations.

7. Network interconnection limitations.

The knowledge of these parameters and their incorporation within the policy distribution decisions, can be used to enhance the network performance, in terms that include communication latency, service delivery/ discovery and autonomy in case of partitioning, since they are correlated with the elements presented at section 8.3.1.

8.3.3 Incorporation of Dynamism

The aforementioned characteristics of the tactical ecosystem, describe a highly dynamic and continuously evolving environment. Thus, the notion of dynamism has to be embodied, not only within the definition of the security policy, but also through the distribution mechanisms. For this reason, the realised security components must incorporate the available dynamic attributes across the network elements/ domains, but also allow for the dynamic security policy evaluation, as presented at section 8.2.

For the purpose of this study, achieving the efficient security policy distribution, also relies on the incorporation of a suitable tactical decision cycle. John Boyd's OODA (Observe, Orient, Decide, Act), is a decision cycle developed and used by military strategists, primarily within the strategic domain and the first two stages (preparation, execution) of combat operations, with additional applications to the third stage (debrief/ evaluation). Evaluating the various suggested iterations of the OODA loop [9], the NCW targeted OODA model, proposed by Smith [45], emerged as the most suitable solution for tactical SOA, despite its complexity. Our decision was promoted by the fact that this model can coincide with suitably adjusted ontologically structured security policies, into the representation of complex and dynamic systems, providing in addition an enhanced level of granularity.

Similarly to the implementations within the strategic domain, the distinction between the involved processes (observe, orient, decide, act) and further segmentation to the defined domains (physical, information and cognitive in Smith's model), can be eminently beneficial towards the technical implementation of a suitable distribution mechanism, within the tactical domain. Thus, the execution of the distinct processes of the decision cycle, can be delegated and distributed within the nodes of each operational group, allowing them to cooperatively reach the attainment of each objective, while dispensing the computational and overall cost. Additionally, the distribution of the involved processes, dispenses the required resources and time for the achievement of the optimality point, within the *Time Cost of Information* and *Decision Confidence/ Quality* function, as described by Harrison [21].

8.4 Accommodation of the Defined Constraints for Security Policy Distribution

Having defined the overall security architecture and the critical parameters, for the distribution of security policies over tactical SOA, it is necessary to reconstruct the framework presented in figure 8.1, in accordance to the aforementioned criteria. This will allow the required minimization of the local policy scope in each tactical node, maintaining all the requisite functionalities. Additionally, this procedure will provide a transformation into a problem similar in nature to a 0-1 multiple knapsack problem, therefore subject to existing and widely studied optimization mechanisms. Furthermore, the incorporation of the identified elements, prior to the implementation of these mechanisms, will significantly increase the computational efficiency, due to the induced minimization of the number of instances.

Aiming to continuously support the required functionalities, within the defined security mechanisms:

1. Capabilities may span across various domains.
2. Actions may span across various capabilities.
3. A specific action within the context of different capabilities or domains, may be governed by a distinct set of rules.

Thus, a three dimensional space is required, in order to represent all the possible combinations of domains, capabilities and actions. The multitude of these ordered triplets constitutes the overall security policy of the tactical network, as presented in figure 8.5, while every individual action can be represented by a vector:

Equation 8.1:
$Action : A'_m = (D\hat{i} + C\hat{j} + A\hat{k}),\ where\ \hat{i}, \hat{j}, \hat{k}\ are\ unit\ vectors.$
as presented in figure 8.6

Due to the aforementioned constraints, mere replication of the entire security policy across all the deployed nodes is not sufficient. The incorporation of node operational specialization (third identified element - table 8.1), can provide an initial filtering, towards the minimization of the distributed policy branches. Thus, the specific operational contexts of the various deployed groups of nodes, correspond to a distinct set of basic vectors (Linearly independent), in the form:

Equation 8.2:
$Security\ policy : SpOg_{(x)} = \{A'_m, A'_{m+1},\ \dots, A'_{m+n}\}$

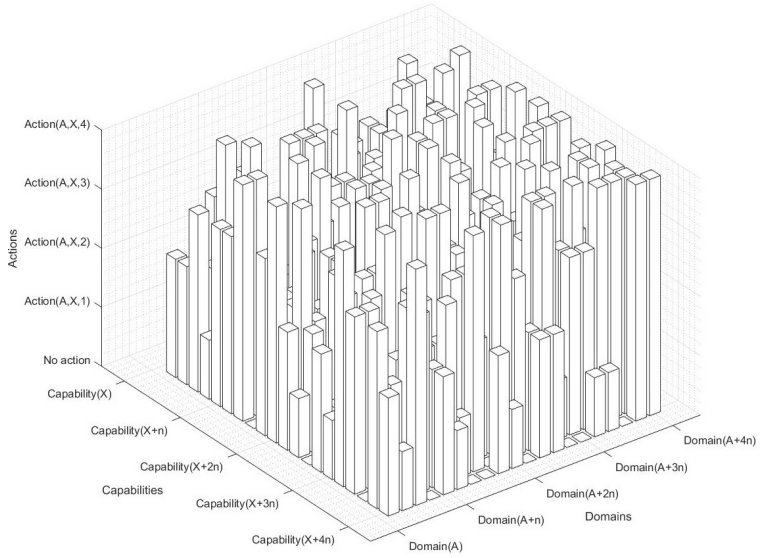

Figure 8.5: Visualisation of a simplified security policy

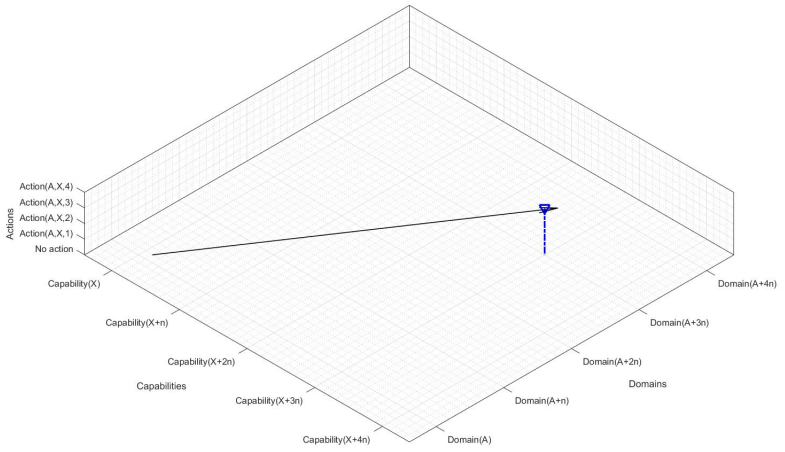

Figure 8.6: Visualisation of a distinct action within the security policy

This mapping is based on the required/ estimated actions of each operational group, within each tactical operation, while it can be constructed a priori and automatically recalled when needed. For instance, a convoy operation may incorporate various operational groups including but not limited to the convoy, multiple protection groups and a medical evacuation group. The structure of the corresponding security policies, for each operational group, has a form similar to those presented in figure 8.7.

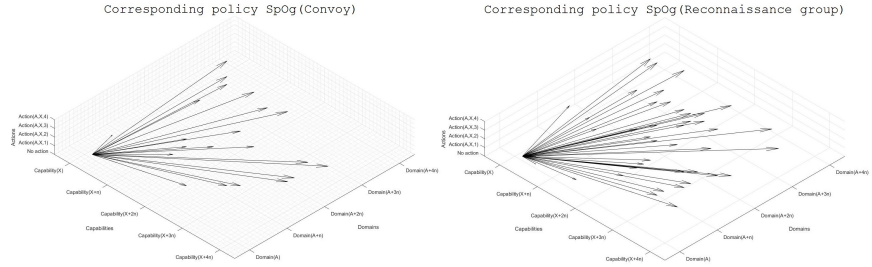

Figure 8.7: Specimen security policy vector sets for convoy and reconnaissance operational groups

Yet, policy replication within an operational group is not the optimal solution, due to the node functional specialization (fourth identified element - table 8.1). Thus, the distinction between the functional groups of nodes across each given operational group, allows for further partitioning of the security policy as:

Equation 8.3:
$SpOg_{(x)} = SpFg_{(y)} \cup SpFg_{(y+1)} \cup ... \cup SpFg_{(y+n)}$

Hence, the security policy of a given operational group is defined as the union of the security policies of the functional groups that constitute it. This allows for the defined subsets ($SpFg_{(y)}$), to collectively compose or address distinct dimensions of the given $SpOg_{(x)}$. Yet, a given vector (Action : $A'_m = (D\hat{i}+C\hat{j}+A\hat{k})$) can span various subsets ($SpFg_{(y)}$) or be unique to one of them. A calculation of the sets intersections (e.g. $SpFg_{(y)} \cap SpFg_{(y+1)}$) and the sets differences (e.g. $SpFg_{(y)}/SpFg_{(y+1)}$), can provide a direct mapping between each action vector and the functional groups, across which it can be distributed, as:

$$\begin{array}{lll} SpFg_{(y)} = \{A'_1, A'_2, A'_3\} & & A'_1 : Fg_{(y)}, Fg_{(y+1)} \\ SpFg_{(y+1)} = \{A'_1, A'_3\} & \succ & A'_2 : Fg_{(y)}, Fg_{(y+2)} \\ SpFg_{(y+2)} = \{A'_2, A'_3, A'_4\} & & A'_3 : Fg_{(y)}, Fg_{(y+1)}, Fg_{(y+2)} \\ & & A'_4 : Fg_{(y+2)} \end{array}$$

As presented in the defined security policy framework (figure 8.1), each vector $A'_m = (D\hat{i} + C\hat{j} + A\hat{k})$ corresponds to a set of governing rules, distinct for each individual action, enabling the dynamic adaptation of the security policy to alterations of the environmental conditions:

Equation 8.4:
$A'_m = \{R_{(z)}, R_{(z+1)}, \ \dots \ , R_{(z+n)}\}$

Each rule is constructed making use of the expressive power of description logic, in order to incorporate the available static and dynamic attributes (sixth identified element - table 8.1) across the network, into the defined security policy decisions. Furthermore, as presented at section 8.3.1, each rule caries an inherited complexity based on the values of the presented metrics, as a function of its syntactic and structural complexities (first and second identified elements - table 8.1). Thus:

Equation 8.5:
$Vector\ complexity : CA'_m = \sum_{z=1}^{n} CR_{(z)}$

Consequently, based on the operational features of the tactical nodes constituting each functional group (fifth identified element - table 8.1), suitable metrics incorporating their computational capacity (e.g. $CCFg_{(y)}$) can be constructed. Hence, given the aforementioned scenario, it is possible to construct a corresponding set of equations among the defined CA'_m and $CCFg_{(y)}$, as:

Equation 8.6:
$CA'_1 = a * CCFg_{(y)} + b * CCFg_{(y+1)}$
$CA'_2 = c * CCFg_{(y)} + d * CCFg_{(y+2)}$
$CA'_3 = e * CCFg_{(y)} + f * CCFg_{(y+1)} + g * CCFg_{(y+2)}$
$CA'_4 = h * CCFg_{(y+2)}$
$a + c + e = 1$
$b + f = 1$
$d + g + h = 1$

If the evaluation of the occurring equations is not feasible or a simplification of the process is required, assumptions can be made regarding the values of the variables, given the incorporation of the two additional identified elements of our study, namely:

1. Dynamic policy evaluation (seventh identified element - table 8.1): Meaning that the most suitable of the *available* rules, is dynamically selected to govern an action.

2. Decision cycle (eighth identified element - table 8.1): Meaning that i) gathering/storing the required rule inputs, ii) selecting the most suitable rule, iii) evaluating the selected rule, iv) enforcing the rule outcome, can be further distributed among the nodes constituting each functional group.

Thus, allowing for some additional flexibility regarding the exact values.

The utilization of the identified elements, as presented in this section, significantly limits the scale of the security policy distribution requirement, by identifying the maximum set of nodes responsible for a given set of actions (equivalently: minimizing the set of actions each node is responsible for). Having introduced the notions of CA'_m and $CCFg_{(y)}$, this has been limited to a problem similar in nature to a 0-1 knapsack problem in the following form.

Given for an action vector $A'_m = \{R_{(1)}, R_{(2)}, ..., R_{(n)}\}$ a finite set of rules, defined so:

$$CR_{(1)} \leq CR_{(2)} \leq, ..., \leq CR_{(n)}$$

and

$$SpFg_{(y)} = \{SpFg_{(1)}, SpFg_{(2)}, ..., SpFg_{(k)}\}$$

a finite set of functional groups of tactical nodes with fixed capacities:

$$CCFg_{(y)} = \{CCFg_{(1)}, CCFg_{(2)}, ..., CCFg_{(k)}\}$$

(calculated earlier as a percentage of their overall CC, dedicated to this action) and fixed 'k'. Assign each element of A'_m across the elements of $SpFg_{(y)}$ so:

1. The capacity of no element of $SpFg_{(y)}$ is exceeded.

2. No element of A'_m is duplicated within any given element of $SpFg_{(y)}$.

3. Duplicates of the elements of A'_m with minimum complexity, are allowed across the elements of $SpFg_{(y)}$, to increase redundancy.

Thus, given that:

1. $pR_{(j)}$=Profit form $R_{(j)}$ (Requirement for a specific subset of rules).
2. $CR_{(j)}$=Complexity of $R_{(j)}$.
3. $CCFg_{(i)}$= The calculated percentage of each CC dedicated to this action.

Then maximize:

Equation 8.7:
$D = \sum_{i=1}^{k} \sum_{j=1}^{n} pR_{(j)} * X_{ij}$

Subject to:

Equation 8.8:
$\sum_{j=1}^{n} CR_{(j)} * X_{ij} \leq CCFg_{(i)}, \;\; i = [1, ..., k]$

Equation 8.9:
$\sum_{j=1}^{n} X_{ij} = 1, \;\; i = [1, ..., k]$

Equation 8.10:
$X_{ij} = 1 \; or \; 0, \;\; i = [1, ..., k], j = [1, ..., n]$

where:

$$X_{ij} = \begin{cases} 1 \text{ if } R_{(j)} \text{ is selected for } Fg_{(i)}, \\ 0 \text{ if not} \end{cases}$$

A variety of exact and heuristic algorithms has been developed for the attainment of optimal/ near optimal solutions for this type of problems [51, 3, 17, 40, 4, 18, 19, 32, 52, 54]. The average solution time of these algorithms is directly correlated to the number of instances [11, 42], which with the incorporation of the defined parameters, has been limited to a minimum set of rules for each node, maintaining at the same time support of all the required functionalities within a tactical operation.

It must also be stated that the described procedure is executed at the mission preparation stage, facing no computational, time, communication or other type of limitations. In this manner, we can achieve a mapping between the required and the available computational power achieving optimal policy partitioning and distribution, incorporating all the corresponding elements of significant impact.

8.5 Conclusions

Through this article, the findings of our study regarding the parameters governing the partitioning and distribution of security policies within tactical SOA, have been presented. Evaluating the characteristics of tactical networks and utilized actors, the involved elements of critical impact, have been identified and analysed. Furthermore, a suitable mechanism has been suggested, accommodating the identified parameters, for the optimum partitioning and distribution of security policies within the mission preparation stage.

Our future plans include the further refinement and evaluation of the proposed mechanism for the mission preparation stage and its extension within the mission execution stage, in the presence of additional constraints, such as connectivity and bandwidth availability. More precisely the utilisation of hierarchical structures within the defined rule sets, governing the individual actions, and the constrained optimization for online distribution of both security policies and governing conditions. Furthermore, we intent to identify suitable mechanisms for the reconciliation of security policies, adjusted to the dynamics of tactical SOA.

Acknowledgments

The results described in this work were obtained as part of the European Defence Agency project TACTICS (Tactical Service Oriented Architecture). The TACTICS project is jointly undertaken by Patria (FI), Thales Communications & Security (FR), Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE (DE), Thales Deutschland (DE), Finmeccanica (IT), Thales Italia (IT), Norwegian University of Science and Technology (NO), ITTI (PL), Military Communication Institute (PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980.

Bibliography

[1] Nato Architecture Framework, NATO Capability View, NAF v3 NCV-2 , June 2013. Available from: http://nafdocs.org/c1-enterprise-classification-2/. 166

[2] ALBERTS, D. S., AND HAYES, R. E. *Power to the Edge: Command and Control in the Information Age* . Information Age Transformation Series. Command and Control Research Portal, 2003. 42, 165

[3] BALAS, E., GLOVER, F., AND ZIONTS, S. An additive algorithm for solving linear programs with zero-one variables. *Operations Research 13*, 4 (1965), pp. 517–549. Available from: http://www.jstor.org/stable/167850. 179

[4] BALAS, E., AND MARTIN, C. H. Pivot and complementa heuristic for 0-1 programming. *Management Science 26*, 1 (1980), 86–96. Available from: http://dx.doi.org/10.1287/mnsc.26.1.86. 179

[5] BAR-NOY, A., CIRINCIONE, G., GOVINDAN, R., KRISHNAMURTHY, S., LAPORTA, T. F., MOHAPATRA, P., NEELY, M., AND YENER, A. Quality-of-information aware networking for tactical military networks. In *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (March 2011), pp. 2–7. 13, 83, 165

[6] BECKER, M., AND SEWELL, P. Cassandra: distributed access control policies with tunable expressiveness. In *Policies for Distributed Systems and Networks, 2004. POLICY 2004. Proceedings. Fifth IEEE International Workshop on* (June 2004), pp. 159–168. 84, 143, 165

[7] BEN BRAHIM, M., CHAARI, T., BEN JEMAA, M., AND JMAIEL, M. Semantic Matching of WS-Security Policy Assertions. In *Service-Oriented Computing - ICSOC 2011 Workshops*, vol. 7221 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2012, pp. 114–130. Available from: http://dx.doi.org/10.1007/978-3-642-31875-7_13. 42, 84, 165

[8] BLANCO, C., LASHERAS, J., VALENCIA-GARCIA, R., FERNANDEZ-MEDINA, E., TOVAL, A., AND PIATTINI, M. A systematic review and comparison of security ontologies. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on* (March 2008), pp. 813–820. 84, 165, 189

[9] BRETON, R., AND ROUSSEAU, R. The future of c2 the c-ooda: A cognitive version of the ooda loop to represent c2 activities. topic: C2 process modelling. 173

[10] BURBANK, J. L., CHIMENTO, P. F., HABERMAN, B. K., AND KASCH, W. T. Key challenges of military tactical networking and the elusive promise of manet technology. *IEEE Communications Magazine 44*, 11 (November 2006), 39–45. 13, 64, 83, 165

[11] CACCETTA, L., AND KULANOOT, A. Computational aspects of hard knapsack problems. *Nonlinear Analysis: Theory, Methods & Applications 47*, 8 (2001), 5547 – 5558. Proceedings of the Third World Congress of Nonlinear Analysts. Available from: `http://www.sciencedirect.com/science/article/pii/S0362546X01006587`. 179

[12] CZENKO, M., DOUMEN, J., AND ETALLE, S. Trust management in p2p systems using standard tulip. In *Trust Management II*, Y. Karabulut, J. Mitchell, P. Herrmann, and C. Jensen, Eds., vol. 263 of *IFIP The International Federation for Information Processing*. Springer US, 2008, pp. 1–16. Available from: `http://dx.doi.org/10.1007/978-0-387-09428-1_1`. 84, 143, 165

[13] DAMIANOU, N., DULAY, N., LUPU, E., AND SLOMAN, M. The ponder policy specification language. *Policy 1* (2001), 18–38. 18, 19, 84, 143, 165, 215

[14] ELMASRY, G. F. A comparative review of commercial vs. tactical wireless networks. *IEEE Communications Magazine 48*, 10 (October 2010), 54–59. 12, 42, 83, 165

[15] FERRINI, R., AND BERTINO, E. Supporting RBAC with XACML + OWL. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT '09)* (Stresa, Italy, June 2009), B. Carminati and J. Joshi, Eds., ACM Press, pp. 145–154. 84, 165, 214

[16] FININ, T., JOSHI, A., KAGAL, L., NIU, J., SANDHU, R., WINSBOROUGH, W. H., AND THURAISINGHAM, B. ROWLBAC - Representing Role Based Access Control in OWL. In *Proceedings of the 13th Symposium on Access control Models and Technologies* (Estes Park, Colorado, USA, June 2008), ACM Press. 84, 143, 165, 189

[17] FRVILLE, A. The multidimensional 01 knapsack problem: An overview. *European Journal of Operational Research 155*, 1 (2004), 1 – 21. Available from: http://www.sciencedirect.com/science/article/pii/S0377221703002741. 179

[18] GAVISH, B., AND PIRKUL, H. Efficient algorithms for solving multiconstraint zero-one knapsack problems to optimality. *Mathematical Programming 31*, 1 (1985), 78–105. Available from: http://dx.doi.org/10.1007/BF02591863. 179

[19] GILMORE, P. C., AND GOMORY, R. E. The theory and computation of knapsack functions. *Operations Research 14*, 6 (1966), pp. 1045–1074. Available from: http://www.jstor.org/stable/168433. 179

[20] GKIOULOS, V., AND WOLTHUSEN, S. D. Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks. *Norwegian Information Security Conference - NISK* (2015), 109–120. 43, 63, 103, 113, 122, 123, 143, 166, 168, 189, 191, 213, 218, 220

[21] HARRISON, F. *The Managerial Decision-Making Process-5th Edition*. South-Western College Pub, 1998. 173

[22] HELIL, N., AND RAHMAN, K. Extending xacml profile for rbac with semantic concepts. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on* (Oct 2010), vol. 10, pp. V10–69–V10–74. 84, 165, 214

[23] HORNE, G., AND LEONARDI, M. *Maneuver Warfare Science 2001*. Marine Corps Combat Development Command, 2001. 42, 83, 165

[24] IST-090 TASK GROUP. Service oriented architecture (SOA) challenges for real time and disadvantaged grid (IST-090). https://www.cso.nato.int/Activity_Meta.asp?ACT=1830, April 2014. 42, 83, 165

[25] IST-118 TASK GROUP. SOA recommendations for disadvantaged grids in the tactical domain (IST-118). https://www.cso.nato.int/ACTIVITY_META.asp?ACT=2293. 42, 83, 165

[26] JOHNSEN, F., BLOEBAUM, T., SCHENKELS, L., FISKE, R., VAN SELM, M., DE SORTIS, V., VAN DER ZANDEN, A., SLIWA, J., AND CABAN, P. SOA over disadvantaged grids experiment and demonstrator. In *Communications and Information Systems Conference (MCC), 2012 Military* (Oct 2012), pp. 1–8. 42, 83, 165, 214

[27] KAGAL, L., FININ, T., PAOLUCCI, M., SRINIVASAN, N., SYCARA, K., AND DENKER, G. Authorization and privacy for semantic web services. *Intelligent Systems, IEEE 19*, 4 (Jul 2004), 50–56. 84, 143, 165

[28] KOLOVSKI, V., PARSIA, B., KATZ, Y., AND HENDLER, J. Representing web service policies in owl-dl. In *In International Semantic Web Conference (ISWC* (2005), pp. 6–10. 84, 165, 189

[29] KOLTER, J., SCHILLINGER, R., AND PERNUL, G. Building a distributed semantic-aware security architecture. In *New Approaches for Security, Privacy and Trust in Complex Environments*, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, Eds., vol. 232 of *IFIP International Federation for Information Processing*. Springer US, 2007, pp. 397–408. Available from: http://dx.doi.org/10.1007/978-0-387-72367-9_34. 84, 143, 165

[30] LI, N., MITCHELL, J., AND WINSBOROUGH, W. Design of a role-based trust-management framework. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on* (2002), pp. 114–130. 84, 143, 165

[31] LUND, K., EGGEN, A., HADZIC, D., HAFSOE, T., AND JOHNSEN, F. Using web services to realize service oriented architecture in military communication networks. *Communications Magazine, IEEE 45*, 10 (October 2007), 47–53. 42, 65, 83, 165, 189

[32] MAGAZINE, M., AND OGUZ, O. A heuristic algorithm for the multidimensional zero-one knapsack problem. *European Journal of Operational Research 16*, 3 (1984), 319 – 326. Available from: http://www.sciencedirect.com/science/article/pii/0377221784902868. 179

[33] MAULE, R. W., AND LEWIS, W. C. Security for distributed soa at the tactical edge. In *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE* (Oct 2010), pp. 13–18. 15, 83, 165

[34] MAYOTT, G., SELF, M., MILLER, G. J., AND MCDONNELL, J. S. Soa approach to battle command: simulation interoperability, 2010. Available from: http://dx.doi.org/10.1117/12.851912. 83, 165

[35] MOFFAT, J. Adapting Modeling & Simulation for Network Enabled Operations. Tech. Rep. ADA555784, Defence Technical Information Center, 2011. 42, 165

[36] MOTIK, B., GRAU, B. C., HORROCKS, I., WU, Z., AND FOKOUE, A. OWL2-Profiles OWL 2 Web Ontology Language Profiles (Second Edition). http://www.w3.org/TR/2012/REC-owl2-profiles-20121211/, December 2012. 169

[37] NEJDL, W., OLMEDILLA, D., AND WINSLETT, M. Peertrust: Automated trust negotiation for peers on the semantic web. In *Secure Data Management*, W. Jonker and M. Petkovi, Eds., vol. 3178 of

Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2004, pp. 118–132. Available from: http://dx.doi.org/10.1007/978-3-540-30073-1_9. 84, 143, 165

[38] NGUYEN, V. Ontologies and information systems: A literature survey, 6 2011. Available from: http://hdl.handle.net/1947/10144. 84, 165, 189

[39] OASIS. Oasis security services (saml) tc. Available from: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security. 84, 143, 165, 214

[40] OHKURA, K., IGARASHI, T., UEDA, K., OKAUCHI, S., AND MATSUNAGA, H. A genetic algorithm approach to large scale combinatorial optimization problems in the advertising industry. In *Emerging Technologies and Factory Automation, 2001. Proceedings. 2001 8th IEEE International Conference on* (Oct 2001), vol. 2, pp. 351–357 vol.2. 179

[41] PATEL-SCHNEIDER, P. F., HAYES, P., AND HORROCKS, I. Owl web ontology language semantics and abstract syntax - owl working group, February 2004. Available from: http://www.w3.org/TR/owl-semantics/. 90, 169

[42] PISINGER, D. Where are the hard knapsack problems? *Computers & Operations Research 32*, 9 (2005), 2271 – 2284. Available from: http://www.sciencedirect.com/science/article/pii/S030505480400036X. 179

[43] RAMLI, C. D. P. K., NIELSON, H. R., AND NIELSON, F. The Logic of XACML. *Science of Computer Programming 83* (Apr. 2014), 80–105. 84, 143, 165, 214

[44] SHI, V. Evaluating the performability of tactical communications networks. *Vehicular Technology, IEEE Transactions on 53*, 1 (Jan 2004), 253–260. 42, 83, 165

[45] SMITH, E. A. *Effects Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War*. Center for Advanced Concepts and Technology, 2002. 173

[46] SMITH, E. A. *Complexity, Networking, and Effects-Based Approaches to Operations*. Center for Advanced Concepts and Technology, 2006. 42, 165

[47] SOUAG, A., SALINESI, C., AND COMYN-WATTIAU, I. Ontologies for security requirements: A literature survey and classification. In *Advanced Information Systems Engineering Workshops*, M. Bajec and J. Eder,

Eds., vol. 112 of *Lecture Notes in Business Information Processing*. Springer Berlin Heidelberg, 2012, pp. 61–69. Available from: http://dx.doi.org/10.1007/978-3-642-31069-0_5. 84, 165, 189

[48] SURI, N. Dynamic Service-oriented Architectures for Tactical Edge Networks. In *Proceedings of the 4th Workshop on Emerging Web Services Technology* (New York, NY, USA, 2009), WEWST '09, ACM, pp. 3–10. Available from: http://doi.acm.org/10.1145/1645406.1645408. 42, 65, 83, 165

[49] TRIVELLATO, D., ZANNONE, N., GLAUNDRUP, M., SKOWRONEK, J., AND ETALLE, S. A semantic security framework for systems of systems. *International journal of cooperative information systems 22*, 01 (2013), 1350004. 20, 84, 143, 165, 189, 190, 215

[50] USZOK, A., BRADSHAW, J., JEFFERS, R., SURI, N., HAYES, P., BREEDY, M., BUNCH, L., JOHNSON, M., KULKARNI, S., AND LOTT, J. Kaos policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement. In *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks* (June 2003), pp. 93–96. 143, 165, 215

[51] VENI, K. K., AND BALACHANDAR, S. R. 0-1 multi constrained knapsack problem (01mkp). *International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering 4*, 7 (2010), 1044 – 1048. Available from: http://waset.org/Publications?p=43. 179

[52] VOLGENANT, A., AND ZOON, J. A. An improved heuristic for multidimensional 0-1 knapsack problems. *The Journal of the Operational Research Society 41*, 10 (1990), pp. 963–970. Available from: http://www.jstor.org/stable/2583274. 179

[53] W3C RECOMMENDATION. OWL2-Overview OWL 2 Web Ontology Language Document Overview (Second Edition). http://www.w3.org/TR/2012/REC-owl2-overview-20121211/, December 2012. 169

[54] WEINGARTNER, H. M., AND NESS, D. N. Methods for the solution of the multidimensional 0/1 knapsack problem. *Operations Research 15*, 1 (1967), 83–103. Available from: http://dx.doi.org/10.1287/opre.15.1.83. 179

Chapter 9

Article 3c: Efficient Security Policy Reconciliation in Tactical Service Oriented Architectures

Efficient Security Policy Reconciliation in Tactical Service Oriented Architectures

2nd International Conference on Future Network Systems and Security (FNSS), Paris, 2016, Springer, CCIS, volume 670, pp. 47-61.

Gkioulos, Vasileios Wolthusen, Stephen D.

Abstract

Tactical mobile ad-hoc networks are likely to suffer from highly restricted link capacity and intermittent connectivity loss, but must provide secure access to services. The conditions under which services may be accessed and which security requirements must be maintained will vary dynamically, and local policies will hence change on a per-node basis even when starting from a common baseline such as when nodes obtain new information.

In this paper we describe a mechanism allowing structured security policies to incorporate such local changes but to efficiently reconcile across tactical SOA networks, allowing the derivation of policy decisions as precomputed Horn clauses or directly reasoning over a description logic fragment. This mechanism minimises the communication overhead compared to earlier work whilst maintaining policy integrity, thereby allowing security policies to adapt to resource and network constraints and other local knowledge such as node compromises and blacklisting.

9.1 Introduction

Tactical networks are mobile wireless ad-hoc or mesh networks with frequently severely limited resources and also subject to loss of connectivity owing to aspects ranging from mobility to adversaries jamming. The use of SOA allows nodes to invoke and dynamically configure services depending on factors including service availability. However, whilst nodes in such a network may commence a mission with a consistent security policy and knowledge of the respective local state and environment, this will evolve

over time. A security policy here relies upon a knowledge base for the target domains, node capabilities and constraints, allowing the dynamic inclusion of local state and environmental knowledge for the on-line selection and configuration of security controls. In SOA, this allows the dynamic invocation and orchestration of services, selecting the node for which services or service choreography may be optimal, and which security controls and mechanisms such as protocols and algorithms are required or supported.

Earlier studies [16, 1] investigated tactical SOA, defining suitable protection goals, security requirements and policy design preconditions in consistence to the identified constraints. Such constraints include the required scalability and dynamic adaptation of the security mechanisms, in addition to the inherently requisite support of heterogeneity, functional diversity and cooperativity across the tactical nodes. Ontologies have been identified as a suitable mediator towards the realisation of security requirements in distinct domains. [26, 31, 35, 7, 27, 34]. Extending this paradigm to tactical SOA [15], the aforementioned preconditions have been translated into security structural and functional requirements. These, necessitated the realization of robust yet flexible protection mechanisms, able to dynamically adapt to the environmental alterations, maintaining support over the defined set of security goals. Thus, the same study suggested a security policy framework dedicated to tactical SOA based on Web Ontology Language, as OWL offers the required scalability and distributed operation, providing sufficient expressive power for capturing and reasoning over the underling semantics [25, 12, 6, 32, 29].

Yet, the functional limitations of tactical nodes render the mere replication of security policies infeasible, while the implemented security mechanisms cannot rely on centralised configurations, since continuous connectivity towards a security dedicated entity cannot be reassured. Thus, a mechanism for the efficient distribution of ontologically defined security policies over tactical SOA has been developed earlier [17]. As specified previously, the distributed security policies must be able to adjust and respond to the continuous alterations of the tactical environment, transitioning between consistent states. This necessitates the incorporation of dynamic semantics within the security policy, which can cause local divergences regarding its scope or context. Such divergences can lead to policy inconsistency and node antagonism, affecting network performance in various terms, including service delivery. Thus, the reconciliation of occurring discrepancies among the distributed ontologies is required.

This paper presents our findings in respect to the reconciliation of singular (or a priory mapped in the case of coalition environments) distributed ontological security policies for tactical SOA, focusing on the mission execution stage. The objective of this study is to achieve this, while minimizing the security induced overhead, both in terms of computational complexity and

bandwidth consumption. Section 9.2 presents related work, while at section 9.3 the main concepts of the previously developed tactical policy model are briefly presented. Section 9.4 includes our findings regarding the nature of the occurring divergences, aiming to minimize the complexity of the reconciliation mechanism and the size of transmitted messages. Consequently, section 9.5 presents the functionality of the components constituting such a mechanism (in respect to the content of section 9.4), while section 9.6 includes the formalisation of these ordered functional elements in algorithmic form.

9.2 Related Work

The resolution of heterogeneity by semantic alignment of distinct ontologies corresponds to ontology mapping, which is a mature area of research both for static and dynamic ontologies [14, 36, 5, 13, 19, 8, 11, 9, 30, 18, 10, 24]. Yet, these methodologies are not suitable for the specifics of tactical SOA, since their definition was targeted on dissimilar domains and the corresponding constraints were not addressed. Some of these mechanisms aim to the mapping of distinct ontologies, focusing on creating a linking dictionary which is not necessary in the case of national or coalition operations, regarding the mission execution stage. Additionally, no communication restrictions are considered, requiring multiple transactions or the transmission of the entire ontology. Furthermore, some mechanisms allow residue unresolved divergences, or require the initiation of a complete mapping cycle, either periodically or at any time that a differentiation is detected.

Focusing on military applications, Bakillah et al. [2] provided a flexible semantic mediation mechanism for heterogeneous sensor data. Yet, despite the nature of sensor networks, no communication restrictions have been considered. Furthermore, Besana et al. [4] suggested the incorporation of service choreography statistics, for the minimization of the ontology mapping problem, over open and distributed environments. Yet, the utilization of such mechanisms for security dedicated ontologies, may allow residue or pending divergences that, thought not relevant for a given transaction, can remain unresolved and be subject to adversarial exploitation. Moreover, Trivellato et al. [34] presented a mapping mechanism at the security domain of maritime coalition environments. That study focus on the mapping of not singular but distinct security policies, and due to the nature of maritime nodes dissimilar communication constraints are considered. Finally, Muthaiyah et al. [28] also focus on the security domain of ontology mapping, but the proposed mechanism does not allow operation over distributed and constrained environments, since it requires the exchange of the entire ontology, for every mapping cycle.

Khattak et al. [23, 21, 20, 22] proposed an ontology mapping mechanism where only the altered semantics are exchanged and reconciled by a centralised mapping system. Such an approach has been proven to provide increased reconciliation efficiency, in terms of time and computational power consumption. Thus, adopting this paradigm across tactical SOA, we seek to satisfy the discrete operational (e.g. distributed operation), security (e.g. increased reconciliation confidence) and functional (e.g. bandwidth consumption) requirements, as presented below.

9.3 Security Policy Formulation and Reasoning

In this section the architecture, formal representation and distribution mechanisms for the examined security policies are briefly presented, according to the results of our previous studies [15, 17, 16, 1]. This is crucial for the identification of the components and functionalities, required for the investigated reconciliation mechanism.

9.3.1 Security Policy Architecture

Supporting the requisite functionalities and dynamic service orchestration over tactical SOA, necessitates the fine-grained conceptualization of the constituent network elements, in correspondence to the anticipated processes and operational requirements. Exploiting the expressive power of OWL, such a mechanism can be defined as presented, in small scale, at figure 9.1.

The anticipated processes and requirements are conceptualised by the unambiguous representation of the tactical domains (Such as planning, management, detection and diligence) and operational capabilities (Such as communication, core, inter-domain and application). The intersection of these two elements corresponds to a predefined set of required actions, which can be visualised in a three dimensional space, with a non uniform distribution. Concurrently, each action is governed by a dynamically selected set of prioritized rules. These are constructed with increasing complexity and preciseness, supporting both the cooperative and standalone functionality of the tactical nodes, in conjunction with their functional characteristics and available resources. These rules also incorporate and serve as links towards the aforementioned static and dynamic properties of the constituent network elements (Namely services, information, network, radios, nodes and subjects).
Thus:

Equation 9.1:
$Individual\_Domain \cap Individual\_Capability = \{Individual\_Action(k), Individual\_Action(k+1), ..., Individual\_Action(k+i)\}$

Where:

Equation 9.2:
$Individual\_Action(k) \widehat{=} \{Individual\_Rule[k(z)], Individual\_Rule[k(z+1)]$
$, ..., Individual\_Rule[k(z+j)]\}$

And:

Equation 9.3:
$$Observable\_Objects \xrightarrow{Indivi.\_Rulek(z)} Governing\_Mechanisms_{Individual\_Action(k)}$$

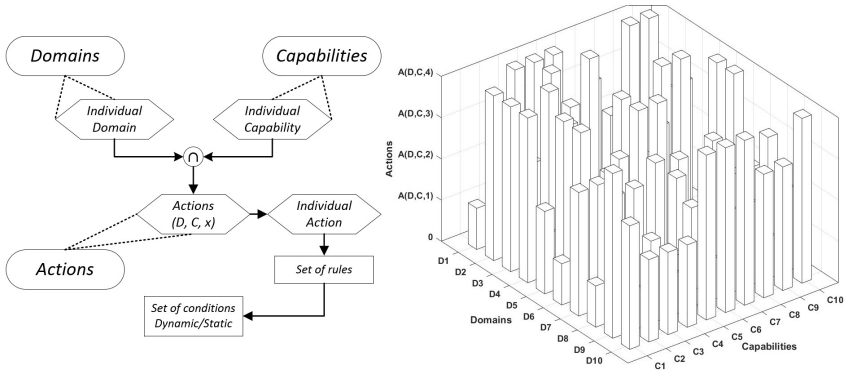

Figure 9.1: Outline of security policy structure.

9.3.2 Formal Representation

The formal representation of the aforementioned elements is achieved with the utilization of the constructors, provided by the selected description logic fragment for the formulation of appropriate unary and binary predicates. In order to achieve precise capturing of the required concepts, the selected DL-fragment must be based on *ALC*, but also support role hierarchies and inclusion, inversion, nominals, functionality properties and qualified cardinality restrictions. *SHOIN(D)* has been identified as a suitable DL-fragment, but more lightweight fragments can also be utilised for optimization purposes. The tactical terminology is constructed within the corresponding T-box, in terms of acyclic and unique concept definitions, as a set of sufficient and necessary conditions. Consequently, constructing expressions similar to those presented at equations 9.4, 9.5 and 9.6, allows to exploit the expressive power of DL in order to gradually structure all the individual concepts, across the distinct tactical domains.

Equation 9.4:
$Terminal \equiv individual \sqcap \exists has\_Terminal\_ID.\ \bot$

Equation 9.5:
$Local\_Provider \equiv Terminal \sqcap \exists Has\_Operational\_Group.OG2$
$\sqcap \exists Has\_Status.Online \sqcap \exists Has\_Functionality.SP$

Equation 9.6:
$Available\_Service \equiv Service \sqcap \leq 1 Has\_Local\_Provider$

Additionally, A-box is oriented to instance identification, where concept and role assertions are utilized in order to specify a given individual as an instance of a specific concept, as presented at equations 9.7 and 9.8.

Equation 9.7:
$Concept\ assertion$
$File \sqcap Video(Message\_x) : Message\_x\ is\ a\ video\ file$

Equation 9.8:
$Role\ assertion$
$hasSource(Message\_x, Terminal\_y) : Terminal\_y\ is\ the\ source\ of$
$Message\_x$

9.3.3 Partitioning and Distribution

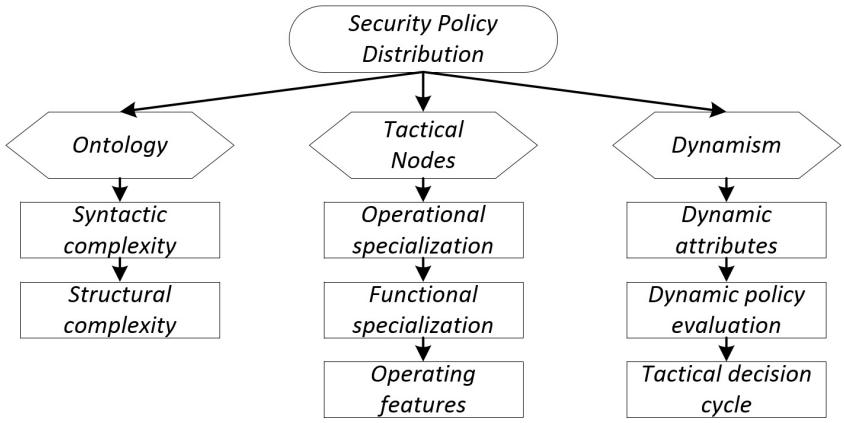

Figure 9.2: Governing parameters of security policy distribution, over tactical SOA.

Assuming a tactical security policy, the efficient distribution of the corresponding ontological structure across the deployed actors, requires the evaluation of various network and operational parameters, as presented in figure 9.2. Incorporating these elements into the distribution mechanism at the mission preparation stage, allows the responsibility allocation for the required actions of a given tactical operation, taking under consideration the structure of the policy, the characteristics and expected behaviour of the tactical nodes, alongside the required dynamic functionalities. This allows the minimization of the policy responsibility overlap across the deployed actors, maintaining their capacity for standalone operation.

Thus, evaluating the syntactic and structural complexity of the ontological structure, in combination with the incorporated dynamic attributes, allows its partitioning and distribution across various node groups, organised based on their required operational/ functional behaviour and their operating features. Additionally, the incorporation of dynamic policy evaluation mechanisms and a tactical decision cycle, allows the extended partitioning of policy decisions, when they are utilized during mission execution. The security policy distribution is a prerequisite of tactical SOA, but as presented earlier it raises the question of reconciling the occupying divergences.

9.4 The Characteristics of Occurring Divergences

Investigating the nature of occurring divergences, four common types of tactical operations have been analysed and simulated, namely i) Tactical convoy, ii) Reconnaissance Surveillance and Target Acquisition, iii) Intervention patrol and iv) Medical Evacuation. Each operation was partitioned into a variety of use cases (e.g. blue force tracking and common operational picture distribution, injection of high mobility nodes, improvised explosive device detection and report, interoperability with police forces) including detailed episodes (e.g. addressed request/ reply, multi-hop service invocation, service discovery and node isolation). This analysis was based on a security policy (see section 9.3) constructed using the DL fragment *ALCHIF(D)* as depicted at figure 9.3, while this core ontological model was adjusted to the specifics of each tactical operation.

Assuming the simplified scenario presented at table 9.2, a divergence at the local knowledge of two nodes (Node_A, Node_B) regarding the status of a sensor attached to a vehicle is presented. In this scenario, during the mission execution stage, hostile forces achieve local prevalence at a given Area of Operation (AoO4), thus the trust level of the locally deployed sensors is automatically degraded. Sensor_09134 is responsible for gathering local blue force tracking data (at the tactical team level), incorporating them into a low resolution local aerial photo and transmitting the output periodically across the network. Node_A becomes aware of the final position

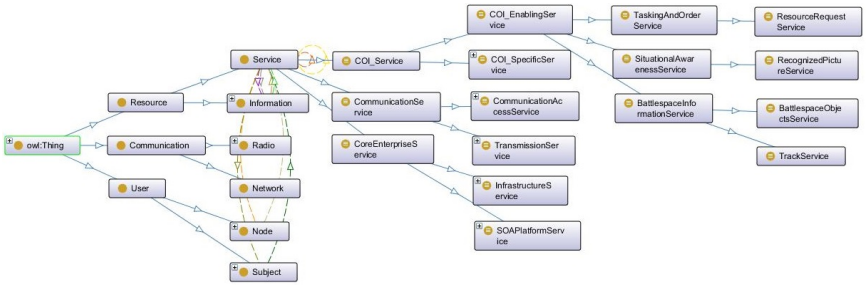

Figure 9.3: Investigated security policy/ontology (Parts of the service subtree are expanded.)

of Sensor_09134 (AoO4) thus limits the trust level according to the security policy, while Node_B maintains the previous update (AoO7) incorporating no alterations and treating information based on the previous status. Similar scenarios can occur in the case of a communication disruption, when a group of nodes (Node_A, Sensor_09134) reconnects with other parts of the network and continues to operate, exchanging information. This scenario refers to a simplified divergence, yet the extent, content and impact of such alterations can vary according to the context of the tactical operation and the structure of the security policy.

Local knowledge at Node_A	**Local knowledge at Node_B**
Information (Message)	Information (Message)
has_Classification(MSG_x, Top_Secret)	has_Classification(MSG_x, Top_Secret)
has_Nature(MSG_x, Blue_Force_Tracking)	has_Nature(MSG_x, Blue_Force_Tracking)
has_Type(MSG_x, Image_jpg)	has_Type(MSG_x, Image_jpg)
has_Size(MSG_x, 200)	has_Size(MSG_x, 200)
has_Source(MSG_x, Sensor_09134)	has_Source(MSG_x, Sensor_09134)
⋮	⋮
Node (Sensor_09134)	Node (Sensor_09134)
has_State(Sensor_09134, Active)	has_State(Sensor_09134, Active)
has_Trust(Sensor_09134, 20)	has_Trust(Sensor_09134, 87)
has_Location(Sensor_09134, AoO4)	has_Location(Sensor_09134, AoO7)
⋮	⋮

Table 9.2: Simplified differentiation scenario from the intervention patrol simulation set.

The results of our analysis can be summarised as:

- Strict syntactic, terminological and semiotic homogeneity is maintai-

- Divergences occur only due to conceptual heterogeneity. This is further restricted since the local ontologies operate within only two dimensions of context dependent representation, namely partiality and perspective, but not in respect to approximation [3]. Hence, minimising granularity negotiations and the corresponding message transmissions.

- Approximation differences are utilized across the defined governing rules of each available action. Thus, it is locally maintained in order to provide dynamic policy adaptation to the tactical network dynamics, without increasing the security induced overhead during multi-party policy reconciliation.

- The elements of the ontological structure that can be affected by such alterations, occur only within the values of defined object and data properties, while their respective ranges and domains remain unaffected. Additional centralized revisions that may require alterations within classes, individuals and SWRL rules, would require a global policy update, which will have to incorporate alternative and more costly mechanisms.

- The type of allowed alterations includes only the modification (revision) of the identified elements, since their extension (addition) or reduction (deletion) would correspond to the privilege allocation to each individual node, of modifying the tactical security policy. Thus, only the revision of the identified elements should be expected and allowed, supporting the adaptation of the extracted policy decisions, based on the evolution of the dynamic semantics across the network.

These findings allow the simplification of the developed reconciliation mechanisms and the minimization of the network resources allocated for this purpose. No terminology or structural negotiations are required, while the divergence targets and types can be considered static. The impact, as visualised at figure 9.4, is located both to the size and complexity of Δ (divergence to be transmitted and reconciled), significantly minimizing the consumption of bandwidth (when treated as transmitted datum) and computational power (when treated as data at rest).

Centralised ontology mapping methodologies require the transmission of the entire ontology either bilaterally to a reconciliation dedicated entity, or unilaterally among the dissident nodes. Change reconciliation based mechanisms provide increased efficiency in terms of elapsed time and computational complexity by referring only to the altered elements. This is achieved by the construction and algorithmic support of a complete ODMT (Ontology Divergence Mapping Tree), as presented in figure 9.4, and the communication of the altered elements in XML or encoded format.

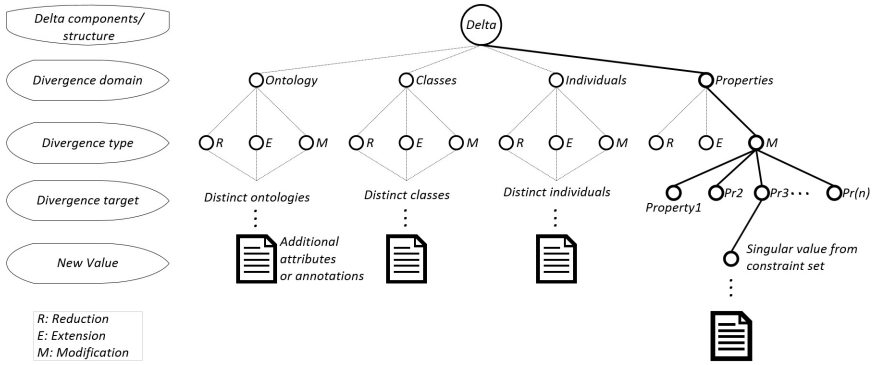

Figure 9.4: Ontology divergence mapping tree.

The presented findings allow further improvement by permitting the reduction of ODMT to the property branch, providing an absolute minimum of Delta components (divergence target + new Value). The satisfaction of network and security requirements necessitates the incorporation of additional attributes and annotations (e.g. divergence source and previous hops ⇛ auditing and non repudiation, Time stamp and precedence ⇛ freshness and prioritization, Divergence trust ⇛ reconciliation confidence). Yet, the initial reduction of ODMT has a significant impact in terms of bandwidth and computational efficiency.

9.5 Identification of Required Elements and Functionalities

The reconciliation of ontologically defined security policies is closely related to ontology mapping mechanisms. Yet, as presented earlier, such solutions are constructed for operation within domains with distinct requirements and constraints to tactical SOA. Zablith et al. [36] described an ontology evolution cycle comprising of five main steps, presenting the corresponding existing mechanisms.

Detecting the need for evolution ⇛ suggesting changes ⇛ validating changes ⇛ assessing impact ⇛ managing changes.

The developed security policy reconciliation mechanism required the addition of a communication step, responsible for the adaptation to the characteristics of tactical SOA. Through the analysis and simulation of the aforementioned tactical operations, the requisite functionalities of the *Communication* step have been identified. Thus, such a mechanism is required to minimize:

- The knowledge propagation time.
- The size of transmitted elements.
- The number of involved nodes.
- The complexity of the transmitted elements.
- The number of interactions.

Additionally, auditing, prioritization and roll back capabilities must be enabled, maintaining increased reconciliation confidence. The presented results regarding the nature of occurring divergences, can be efficiently utilized in order to minimize the size and complexity of transmitted elements, while the additional requirements are attained by the use of appropriately constructed mechanisms.

OWL operates over the open world assumption, which is required by the functional characteristics of the defined security policy. Yet, it is possible to enforce closed world assumption during the construction of the policy by the definition of explicit constraints. Thus, data driven evolution is possible. This can be achieved by recording the Δ caused by the various data sources (services, terminals, users) and initiate the reconciliation either as event driven (a session related policy reconciliation) or when the QoS mechanisms signal that the required resources have become available. The developed mechanisms for the achievement of the aforementioned requirements are:

1. Local ontology (fragment of the global ontology/ policy (section 9.3))
2. Local node assignment list (fragment of a global node assignment list, responsible for the identification of the subset of nodes, which incorporate the altered element.)
3. Local change ontology (maintains a copy of locally sensed and enforced changes for audit and roll back purposes).
4. Criticality/ timeliness measure (for prioritization purposes)
5. Archive of requested changes (maintains a copy of externally requested changes for audit and roll back purposes).
6. Δ (it includes the altered element, and various characteristics of the alteration, such as justification, time, actor.)

The global node assignment list (G-NAL) operates as a responsibility database, used for the initial partitioning and distribution of the security policy across the deployed actors. The local node assignment list is a fragment of G-NAL that during a policy reconciliation at the mission execution stage is used in order to minimise the number of involved nodes and interactions, to the minimum acceptable subset of recipients/ transmitters that provide sufficient reconciliation confidence.

This mechanism has been constructed with minimum complexity using the SF(D) DL fragment, as presented in figure 9.5 with the use of a transitive object property (e.g. Makes_Use_Of) between the deployed assets (nodes), the required actions and the existing object or data properties, providing a mapping between the nodes and the possibly altered attributes. Querying this ontology (e.g. Uses value ServiceStatus and HasOG some string) provides a list of nodes that have to be updated once a change is detected locally (e.g. on the ServiceStatus), or the list of nodes that belong to the same Operational group and are expected to transmit update requests (used for Get_Recipients, Get_Requesters, Get_Properties of Section 9.6).

Additionally, the required criticality and timeliness measures have been attached to the properties of this mechanism, in the form of data properties, in order to provide prioritization of the reconciliation requests in a congested environment. Criticality measures follow military precedence designators as flash (e.g. intrusion detection, compromised node), Immediate (e.g. trust level update), Priority (e.g. local service provider, service registry update) and routine (e.g. location update, service status update). Prior to transmission the extracted set of Δ are initially classified in respect to their criticality (maximum first), and consequently based on their life cycle (minimum first), while the corresponding update requests are transmitted in accordance to the available network resources (used for Sort_Changes of Section 9.6).

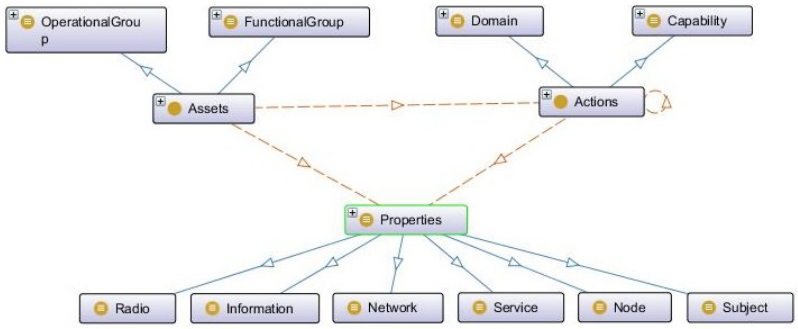

Figure 9.5: Structure of node assignment list.

Khattak et al. [23, 21, 20, 22] presented a flexible and robust mechanism for the construction of the required local change ontology (which is also suitable for the inbound oriented, archive of requested changes), combined with the capability of extracting the required Δ and its use for the mapping of dynamic ontologies. These mechanisms can be modified in order to serve only the identified components, based on the nature of occurring divergences (section 9.4). Thus, being adequately lightweight in order to serve under the tactical constraints and update the locally stored ontologies given a specific Δ (used for Update_Local_Policy of Section 9.6).

9.6 Policy Reconciliation Mechanism

A reconciliation mechanism has been developed based on the presented elements, in order to provide the aforementioned functionalities. The corresponding algorithms for the formalization of the ordered functionality sets are presented bellow.

Transmitter

```
-> Identify that a set of properties evolved locally.
   ↪ Related "Change_Detection" alert coming from a
   ↪ Meta-data Handler or Contextual Monitoring local
   ↪ service.
1> If{Change_Detection == TRUE} then
   -> Incorporate changes into the local security
      ↪ ontology. (Existing mapping mechanisms).
   2> Update_Local_Policy(Δ,Security_Ontology)
   -> Incorporate changes into the local change
      ↪ ontology. (existing mapping mechanisms).
   3> Update_Local_Policy(Δ,Local_Change_Ontology)
   -> Query the local node assignment list for the
      ↪ corresponding list of nodes (as described).
   4> (Recipients_List)Get_Recipients(Δ)
   -> Apply criticality and prioritization measures (As
      ↪  described).
   5> (Δ')Sort_Changes(Δ)
   -> Send to QoS Mechanisms for transmission to the
      ↪ list of recipients.
   6> Send_QoS(Δ', Recipients_List)
7> EndIf
```

Receiver

```
-> Receive the first update request for a specific
   ↪ property.
1> If{Receive_Update_Request.Δ'[x] == TRUE} then
   -> Store changes to archive of requested changes (
      ↪ existing mapping mechanisms).
   2> Update_Local_Policy((Δ'[x]), AoRC)
   -> Query local node assignment list for expected
      ↪ requests. (similarly to Get_Recipients, it
      ↪ provides a list of nodes that belong to the
      ↪ same operational group, thus sensed the
      ↪ property alteration and are expected to
      ↪ transmit similar requests).
   3> (Requester_List)Get_Requesters(Δ'[x])
   -> Query local node assignment list for lifetime and
      ↪  criticality measures of Δ'[x] (as described).
   4> (TΔ'[x], CΔ'[x])Get_Properties(Δ'[x])
   -> Request estimated list of requests from QoS
      ↪ mechanisms. (identify requesters who have the
      ↪ resources to transmit requests within the T
      ↪ Δ'[x]).
   5> (Requester_List')QoS_Estimation(Requester_List, TΔ'[x]
      ↪ )
   -> Wait for the expected update requests.
   6> While{TΔ'[x]!=0} do
            If{Receive_Update_Request.Δ'[x] == TRUE}
               ↪ then
            Update_Confidence.Δ'[x]++
            EndIf
      EndWhile
   -> Incorporate the update.
   7> If{Update_Confidence.Δ'[x] ≥ CΔ'[x]} then
            Update_Local_Policy(Δ'[x],Security_Ontology)
      Else
            Discard(Δ'[x])
      EndIf
8> EndIf
```

The described functions (as analysed in Section 9.5) either return a fixed-length array based on a parameters-request, or perform partial order sorting of a given fixed-length array. The only included loop is time dependent, corresponding to the data property $T\Delta^{'}[x]$ that is also a fixed-length array predefined based on the lifetime of the altered property $\Delta[x]$. The value of $T\Delta^{'}[x]$ monotonically decreases for every execution of the cycle. Hence, both algorithms terminate after the consecutive execution of the required steps,

Regarding the correctness of the algorithms, at the transmitter side applying the constraints identified at section 9.4, allows for the consecutive execution of the required steps, for the update of the local policy and local audit mechanisms, in addition to the transmission of update requests to the required recipients in a prioritized order. At the receivers side with the reception of a non-incorporated alteration, the audit mechanisms are initially updated (AoRC), while the acceptance or rejection of the update request is based on a reconciliation confidence measure, calculated based on the number of estimated requesters. Given an update request, the local security mechanisms provide (through the node assignment list) a group of nodes that are co-located and serve the execution of the same action with the original update requester. Additionally, the local QoS mechanisms limit this list based on the current connectivity measures, providing the final $Requester\_List^{'}$, which includes the nodes that are expected and have the resources to transmit similar requests. If the sum of received requests meets the predefined criticality measure ($C\Delta^{'}[x]$ can correspond to a percentage of $Requester\_List^{'}$), the alteration is accepted, incorporated and forwarded using the transmitter algorithm, otherwise it is recorded and rejected.

9.7 Conclusions

Through this article, the findings of our study regarding the reconciliation of ontologically defined security policies for tactical SOA, during the mission execution stage, have been presented. The primary contributions of this article are the investigation of the possible divergences and the identification of the required functionalities for policy reconciliation. The nature of occurring divergences has been limited to an expected and permitted subset, both in terms of scope, source and subject.

Furthermore, the required functionalities for their reconciliation have been identified, taking under consideration the constraints of the tactical environment and the requirement for auditing, prioritization and roll back capabilities. Additionally, the developed mechanism for the consolidation of the reconciliation requirements and tactical constraints has been presented.

Our future plans include the further investigation and refinement of the proposed mechanism, with the incorporation of service invocation related

metrics, and its extension within the scope of global or extended policy updates. Furthermore, within the scope of the ongoing project TACTICS, the analysis presented in this study and positive initial experimental results, are to be verified and demonstrated in large scale realistic scenarios.

9.7.0.1 Acknowledgments:

The results described in this work were obtained as part of the EDA (European Defence Agency) project TACTICS (Tactical Service Oriented Architecture). The TACTICS project is jointly undertaken by Patria (FI), Thales Communications & Security (FR), Fraunhofer-Institut fur Kommunikation, Informationsverarbeitung und Ergonomie FKIE (DE), Thales Deutschland (DE), Leonardo (IT), Thales Italia (IT), Gjøvik University College (NO), ITTI (PL), Military Communication Institute (PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980 GP.

Bibliography

[1] ALOISIO, A., AUTILI, M., D'ANGELO, A., VIIDANOJA, A., LEGUAY, J., GINZLER, T., LAMPE, T., SPAGNOLO, L., WOLTHUSEN, S. D., FLIZIKOWSKI, A., AND SLIWA, J. TACTICS: TACTICal Service Oriented Architecture. *CoRR abs/1504.07578* (2015). Available from: `http://arxiv.org/abs/1504.07578`. 43, 63, 103, 121, 143, 154, 189, 191, 212

[2] BAKILLAH, M., LIANG, S. H., ZIPF, A., AND MOSTAFAVI, M. A. A dynamic and context-aware semantic mediation service for discovering and fusion of heterogeneous sensor data. *Journal of Spatial Information Science* (2013). 190

[3] BENERECETTI, M., BOUQUET, P., AND GHIDINI, C. On the dimensions of context dependence: Partiality, approximation, and perspective. In *Modeling and Using Context*, V. Akman, P. Bouquet, R. Thomason, and R. Young, Eds., vol. 2116 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2001, pp. 59–72. Available from: `http://dx.doi.org/10.1007/3-540-44607-9_5`. 196

[4] BESANA, P., AND ROBERTSON, D. How service choreography statistics reduce the ontology mapping problem. In *The Semantic Web*, K. Aberer, K.-S. Choi, N. Noy, D. Allemang, K.-I. Lee, L. Nixon, J. Golbeck, P. Mika, D. Maynard, R. Mizoguchi, G. Schreiber, and P. Cudr-Mauroux, Eds., vol. 4825 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2007, pp. 44–57. Available from: `http://dx.doi.org/10.1007/978-3-540-76298-0_4`. 190

[5] BESANA, P., AND ROBERTSON, D. Probabilistic dialogue models for dynamic ontology mapping. In *Uncertainty Reasoning for the Semantic Web I*, P. da Costa, C. dAmato, N. Fanizzi, K. Laskey, K. Laskey, T. Lukasiewicz, M. Nickles, and M. Pool, Eds., vol. 5327 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2008, pp. 41–51. Available from: `http://dx.doi.org/10.1007/978-3-540-89765-1_3`. 190

[6] BLANCO, C., LASHERAS, J., VALENCIA-GARCIA, R., FERNANDEZ-MEDINA, E., TOVAL, A., AND PIATTINI, M. A systematic review and comparison of security ontologies. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on* (March 2008), pp. 813–820. 84, 165, 189

[7] BUNCH, L., BRADSHAW, J., AND YOUNG, C. Policy-governed information exchange in a u.s. army operational scenario. In *Policies for Distributed Systems and Networks, 2008. POLICY 2008. IEEE Workshop on* (June 2008), pp. 243–244. 189

[8] CHOI, N., SONG, I.-Y., AND HAN, H. A survey on ontology mapping. *SIGMOD Rec. 35*, 3 (Sept. 2006), 34–41. Available from: http://doi.acm.org/10.1145/1168092.1168097. 190

[9] COBNA, G., ABDESSALEM, T., AND HINNACH, Y. A comparative study of xml diff tools, 2004. 190

[10] DOS REIS, J. C., PRUSKI, C., AND REYNAUD-DELAÎTRE, C. State-of-the-art on mapping maintenance and challenges towards a fully automatic approach. *Expert Syst. Appl. 42*, 3 (2015), 1465–1478. Available from: http://dx.doi.org/10.1016/j.eswa.2014.08.047. 190

[11] EUZENAT, J., AND SHVAIKO, P. *Ontology matching*, 2nd ed. Springer-Verlag, Heidelberg (DE), 2013. 190

[12] FININ, T., JOSHI, A., KAGAL, L., NIU, J., SANDHU, R., WINSBOROUGH, W. H., AND THURAISINGHAM, B. ROWLBAC - Representing Role Based Access Control in OWL. In *Proceedings of the 13th Symposium on Access control Models and Technologies* (Estes Park, Colorado, USA, June 2008), ACM Press. 84, 143, 165, 189

[13] FLOURIS, G., PLEXOUSAKIS, D., AND ANTONIOU, G. On applying the agm theory to dls and owl. In *In 4th International Semantic Web Conference (ISWC* (2005), pp. 216–231. 190

[14] FUDHOLI, D. H., RAHAYU, W., AND PARDEDE, E. A data-driven dynamic ontology. *J. Inf. Sci. 41*, 3 (June 2015), 383–398. Available from: http://dx.doi.org/10.1177/0165551515576478. 190

[15] GKIOULOS, V., AND WOLTHUSEN, S. D. Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks. *Norwegian Information Security Conference - NISK* (2015), 109–120. 43, 63, 103, 113, 122, 123, 143, 166, 168, 189, 191, 213, 218, 220

[16] GKIOULOS, V., AND WOLTHUSEN, S. D. Securing tactical service oriented architectures. In *2016 International Conference on Security of Smart*

Cities, Industrial Control System and Communications (SSIC) (July 2016), pp. 1–6. 63, 71, 103, 113, 122, 123, 143, 154, 157, 189, 191, 213, 218, 220

[17] GKIOULOS, V., AND WOLTHUSEN, S. D. *Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures*. Springer International Publishing, Cham, 2017, pp. 149–166. Available from: http://dx.doi.org/10.1007/978-3-319-44354-6_9. 43, 63, 103, 113, 114, 122, 123, 143, 189, 191, 213, 218, 223

[18] HEFLIN, J., AND HENDLER, J. Dynamic ontologies on the web, 2000. 190

[19] HOOI, Y., HASSAN, M., AND SHARIFF, A. A survey on ontology mapping techniques. In *Advances in Computer Science and its Applications*, H. Y. Jeong, M. S. Obaidat, N. Y. Yen, and J. J. J. H. Park, Eds., vol. 279 of *Lecture Notes in Electrical Engineering*. Springer Berlin Heidelberg, 2014, pp. 829–836. Available from: http://dx.doi.org/10.1007/978-3-642-41674-3_118. 190

[20] KHATTAK, A., LATIF, K., KHAN, S., AND AHMED, N. Managing change history in web ontologies. In *Semantics, Knowledge and Grid, 2008. SKG '08. Fourth International Conference on* (Dec 2008), pp. 347–350. 191, 200

[21] KHATTAK, A., PERVEZ, Z., KHAN, W., KHAN, A., LATIF, K., AND LEE, S. Mapping evolution of dynamic web ontologies. *Information Sciences 303* (2015), 101 – 119. Available from: http://www.sciencedirect.com/science/article/pii/S002002551401192X. 191, 200

[22] KHATTAK, A. M., LATIF, K., AND LEE, S. Change management in evolving web ontologies. *Know.-Based Syst. 37* (Jan. 2013), 1–18. Available from: http://dx.doi.org/10.1016/j.knosys.2012.05.005. 191, 200

[23] KHATTAK, A. M., PERVEZ, Z., LATIF, K., AND LEE, S. Short communication: Time efficient reconciliation of mappings in dynamic web ontologies. *Know.-Based Syst. 35* (Nov. 2012), 369–374. Available from: http://dx.doi.org/10.1016/j.knosys.2012.04.016. 191, 200

[24] KLEIN, M., PROEFSCHRIFT, A., CHRISTIAAN, M., KLEIN, A., AND AKKERMANS, P. D. J. M. Change management for distributed ontologies. Tech. rep., 2004. 190

[25] KOLOVSKI, V., PARSIA, B., KATZ, Y., AND HENDLER, J. Representing web service policies in owl-dl. In *In International Semantic Web Conference (ISWC* (2005), pp. 6–10. 84, 165, 189

[26] LACY, L., AVILES, G., FRASER, K., GERBER, W., MULVEHILL, A. M., AND GASKILL, R. Experiences using OWL in military applications. In *Proceedings of the OWLED*05 Workshop on OWL: Experiences and Directions, Galway, Ireland, November 11-12, 2005* (2005). Available from: http://ceur-ws.org/Vol-188/sub27.pdf. 189

[27] LUND, K., EGGEN, A., HADZIC, D., HAFSOE, T., AND JOHNSEN, F. Using web services to realize service oriented architecture in military communication networks. *Communications Magazine, IEEE 45*, 10 (October 2007), 47–53. 42, 65, 83, 165, 189

[28] MUTHAIYAH, S., AND KERSCHBERG, L. Dynamic integration and semantic security policy ontology mapping for semantic web services (sws). In *Digital Information Management, 2006 1st International Conference on* (Dec 2007), pp. 116–120. 190

[29] NGUYEN, V. Ontologies and information systems: A literature survey, 6 2011. Available from: http://hdl.handle.net/1947/10144. 84, 165, 189

[30] RANA, V., AND SINGH, G. Mbsom: An agent based semantic ontology matching technique. In *Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference on* (Feb 2015), pp. 267–271. 190

[31] SEMY, S. K., PULVERMACHER, M. K., OBRST, L. J., AND PULVERMACHER, M. K. Toward the use of an upper ontology for u.s. government and u.s. military domains: An evaluation. Tech. rep., Submission to Workshop on Information Integration on the Web (IIWeb-04), in conjunction with VLDB-2004, 2004. 189

[32] SOUAG, A., SALINESI, C., AND COMYN-WATTIAU, I. Ontologies for security requirements: A literature survey and classification. In *Advanced Information Systems Engineering Workshops*, M. Bajec and J. Eder, Eds., vol. 112 of *Lecture Notes in Business Information Processing*. Springer Berlin Heidelberg, 2012, pp. 61–69. Available from: http://dx.doi.org/10.1007/978-3-642-31069-0_5. 84, 165, 189

[33] STOJANOVIC, M. S. L., DR, P., STUDER, R., AND (TH, U. K. Methods and tools for ontology evolution. Tech. rep., 2004. 195

[34] TRIVELLATO, D., ZANNONE, N., GLAUNDRUP, M., SKOWRONEK, J., AND ETALLE, S. A semantic security framework for systems of systems. *International journal of cooperative information systems 22*, 01 (2013), 1350004. 20, 84, 143, 165, 189, 190, 215

[35] USZOK, A., BRADSHAW, J., LOTT, J., JOHNSON, M., BREEDY, M., VIGNATI, M., WHITTAKER, K., JAKUBOWSKI, K., BOWCOCK, J., AND APGARD, D. Toward a flexible ontology-based policy approach for network operations using the kaos framework. In *MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011* (Nov 2011), pp. 1108–1114. 189

[36] ZABLITH, F., ANTONIOU, G., D'AQUIN, M., FLOURIS, G., KONDYLAKIS, H., MOTTA, E., PLEXOUSAKIS, D., AND SABOU, M. Ontology evolution: a process-centric survey. *The Knowledge Engineering Review 30* (1 2015), 45–75. Available from: `http://journals.cambridge.org/article_S0269888913000349`. 190, 197

Chapter 10

Article 4a: TACTICS: Validation of the Security Framework Developed for Tactical SOA

TACTICS: Validation of the Security Framework Developed for Tactical SOA

Journal of Information Security and Applications, 2017, Elsevier, volume 35, pp. 96-105.

Gkioulos, Vasileios Erko Risthein Wolthusen, Stephen D.

Abstract

Contemporary military networks and the requirements arising from future strategic planning, call for the increasing integration of information mobility and network enabled capabilities on the field. Therefore, adopting SOA concepts for the development of command and control infrastructures have become essential, since they provide modularity, flexibility and interoperability of services. Nevertheless, constraints related to infrastructure and operational aspects, render current enterprise SOA ineffective for the tactical domain. Accordingly, the goal of TACTICS was the definition and experimental demonstration of a TSI that enables contemporary tactical radio equipment to participate in SOA, providing the required functionalities under the imposed constraints. This article presents a comprehensive view of the developed architecture, focusing on the elements that constitute the security framework according to our closing experimental results and field demonstrations.

10.1 Introduction

According to the experience gained from the battlefields of the last decade, the requirements for future strategic planning include the increased integration of NEC and NCW at the tactical edge. This is expected to improve situational awareness and reactivity within the developed C2 and C4I systems, by integrating information, information sources, services, decision makers and actors under a dynamically adjustable framework [22, 2, 20, 21, 19, 6].

Therefore, the scope of TACTICS, as described earlier [1], is to enable this through the definition and experimental demonstration of a TSI compatible

with the constraints of tactical networks, that would allow contemporary network components to support operational services within the tactical environment. As presented in the aforementioned article, current enterprise SOA are not suitable for the tactical edge, since they either depend on centralised configurations, or they are not adjusted to the constraints imposed by the tactical domain. Accordingly, TACTICS explicitly focused on such constraints, aiming initially to provide a proof of concept for the capacity to deploy SOA at the tactical edge, and consequently to develop a unified TSI for the participating nations, tailored to the defined requirements.

The TACTICS TSI has been defined as a transparent middle-ware between the information and radio access subsystems. This middle-ware has been vertically divided into two parallel service stacks, called *Processing Pipeline* and *Controller*. The services across the processing pipeline are responsible for message processing, as these messages are forwarder bilaterally between the information system and the radio access system. Such processing adaptations occur at three distinct levels namely service, message, and packet. Additionally, the services across the controller are responsible for the supervision of the functionalities executed within the processing pipeline, the collection of cross-layer information (by monitoring messages and services), and for triggering required adaptations of the systems behaviour.

Under this scope, the security related studies within TACTICS followed four consecutive steps. Initially, the operational constraints and security requirements of such a system have been identified, focusing both on information communication or storage [10], and on information processing in respect to the service components [14]. Consequently, suitable lightweight enforcement mechanisms have been identified, aiming to accommodate the requirements extracted from the aforementioned studies. These mechanisms (e.g. algorithmic implementations of integrity protection frameworks) have been selected according to a state of the art review for currently available open access solutions. Therefore they constitute consortium recommendations but not architectural components of the developed TSI, since they are expected to be replaced by tailored national implementations.

In terms of the architectural components, the third major step of our study referred to the identification of a suitable security policy mechanism for the targeted environment [8]. Analysing the characteristics of tactical networks and operations, allowed the identification of functional requirements for the developed security policy infrastructure. Furthermore, an extensive state of the art review revealed divergences between the capacity of existing policy frameworks and the identified requirements for future tactical networks. Therefore, a tailored solution has been developed based on semantic web technologies, aiming to accommodate the requirements and constraints imposed by tactical SOA [12, 9, 11].

Finally, the fourth step of our study referred to the design and development of the security related components within the TACTICS TSI. These refer to six core services responsible for the security policy governance, and a set of functional services that correspond to the aforementioned enforcement mechanisms [34, 13]. The core services constitute the architectural components of TACTICS TSI, while the functional services are expected to be replaced by tailored national implementations. Nevertheless, the corresponding functionalities and interfaces have been defined, in order to accommodate the required modularity and separation of duty.

This article presents a comprehensive view of these four elements, summarising the security related results within the TACTICS TSI. Therefore, the focus of this article is to present additional architectural details, in respect to the development and supported functionalities. For this purpose, section 3 presents the operational context under which the developed architecture was evaluated, by the execution of simulations at the initial stages of our study and consequently by laboratory and field experiments/ demonstrations. The subsequent sections present a sub-set of the supported functionalities, following one of the developed validation scenarios for the TACTICS closing demonstration. Through this scenario, we seek to highlight how the elements presented in the aforementioned studies, are developed and combined towards supporting future SOA implementations at the tactical edge.

10.2 Related Work

In recent years, SOA based solutions for military networks have become a very active research area [23, 24, 18, 28, 3], due to the benefits promised by SOA, and their successful deployment across enterprise environments. Nevertheless, the existing technologies and standards are not suitable for the highly constrained tactical environments. The MIDNET [17] project from EDA, was focused on facilitating stable communication over disrupted networks. The developed architecture and services allowed the definition of a disruption tolerant design, through a cross layered approach. Furthermore, at ACM [30] the network traffic is adjusted to current conditions, by utilising an enhanced middle-ware and publish/subscribe service.

Moreover the NATO STO/ IST-090 and STO/ IST-118 research task groups focused on the analysis and adaptation of SOA solutions for the tactical edge [16, 29]. Identifying the constraints of the tactical environment, the executed studies concluded that enterprise SOA, including those developed for the military strategic domain, are not suitable for the tactical edge. Outcomes from these studies that relate with TACTICS, refer to the necessity for traffic adaptation, and dynamic cross layer optimization. Focusing on security, earlier studies over tactical SOA, focused primarily on the adaptation of widely used frameworks, such as XACML [27, 15, 7], SAML [25],

WS-Security [26], KAoS [33] and Ponder [4]. Yet, as identified through our early studies, and summarised by Trivelato et al. [32], such frameworks are not suitably adjusted to the requirements of the tactical domain, therefore necessitating the development of tailored solutions.

10.3 Operational Context of Validation Scenarios

The validation scenarios for TACTICS are placed in a fictional region called "Obsidia", which has been defined as a failed multi-ethnic state, on which a multinational task force has been authorised with a peacekeeping operation. Obsidia is dimensioned as a 250km by 200km area, and consists of three autonomous regions, namely Goodlandia, Roguestate and Lakelandia, as presented in Figure 10.1. Goodlandia borders Roguestate to the north, with the mixed population region called "Provincial state" being the major source of conflict between the two. The largest city across Obsidia is "Harbour city" that serves as a supply center for the entire region, as well as the operational base for the Obsidia task force (OTF). Consequently, many central routes lead from Harbour city to the various Goodlandia border settlements across the Provincial state and towards "Lake central".

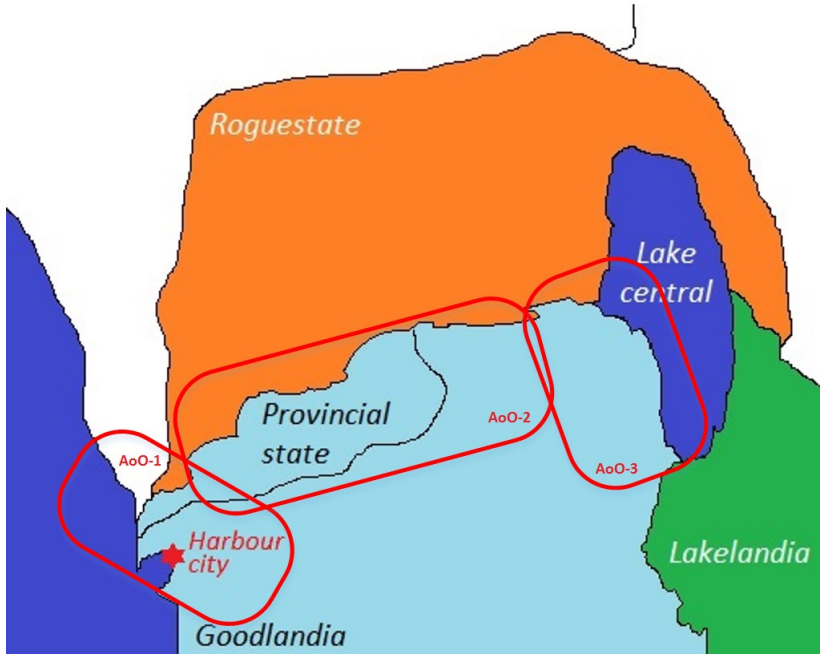

Figure 10.1: The Obsidia region.

The sources of conflict between Goodlandia and Roguestate originate from the attempts of the later to exploit the local mixed population, aiming to annex the Provincial state region in order to seize local resources and obtain direct access to the sea. Additionally, various minor disputes exists across the borders, including the apportionment of Lake central. The Roguestate local government recruited and armed a group of insurgents tasked with destabilizing the Provincial state, while simultaneously disturbing governmental and safety operations across Goodlandia. Following armed attacks against Goodlandian police and military forces, as well as the declaration of a self-ruled independent region across the Provincial state, OTF has been deployed by the United Nations in order to oppose the insurgents and establish a demilitarized zone.

The OTF established three AoO across the borders. AoO-1 controls the access to the Harbour city and provides the required facilities for the OTF-Head Quarters, with close proximity to the local government and police forces. Harbour city and the surrounding area has been targeted by the insurgents under covert operations, with use of IEDs and long range weapons. AoO-2 includes the majority of the Provincial state and border line between Goodlandia and Roguestate. A Goodlandian battle-group, OTF forces and some allied combat service support organizations have been allocated for the protection of the area. Yet, insurgent activity is escalating under the support of the Roguestate armed forces. Finally, AoO-3 is under the control of a coalition of Goodlandian, Lakelandian and OTF forces with unobstructed governance and infrastructure. The only enemy activity in the area is the limited transportation of troops and resources through the borders towards AoO-2. Yet, major towns across Lake central require to be supplied from Harbour city.

This operational context has been utilized within TACTICS for the establishment of refined test-cases and scenarios, incorporating a variety of tactical operations towards the validation of the developed tactical service oriented architecture. The designed tactical service infrastructure was targeted towards the satisfaction of 107 requirements (60-MUST priority, 40-SHOULD priority, 7-COULD priority) referring to 21 distinct aspects (e.g. configuration flexibility, network monitoring, service delivery, routing and quality of service), including 34 security related requirements. The aforementioned scenarios have been utilized through TACTICS, for the development and execution of the theoretical studies and simulations, extending to field and laboratory demonstrations with the use of contemporary tactical radio equipment.

In the following sections we present specific episodes from one of the developed scenarios for the aforementioned demonstrations, aiming to highlight a selected subset of the functionalities supported by the developed tactical SOA security architecture. It must be noted that the majority of TSI

functionalities (e.g. QoS, service registry/discovery, messaging, routing) involved in this test-case have been removed or simplified in the presentation of those episodes, in order to highlight the security related aspects for the purposes of this article. The presented functionalities include:

i. Capturing and incorporation of fine-grained network semantics of static and dynamic nature across the security policy.
ii. Fine-grained action governance/definition, according to the developed (Domain $\longmapsto$ Capability $\longmapsto$ Action) paradigm.
iii. Definition of prioritized rule set per action, according to the developed paradigm.
iv. Scalability of policy and service architecture, and ability to transition between distinct policy fragments.
v. Adaptability to rapid network alterations.
vi. Ability to substitute actions on-line (In a prioritized manner).
vii. Standalone node operation.
viii. Ability to transition between governing rules, and fall back operation.
ix. Incorporation of pre-computed policy decisions.

The selected test-case refers to a convoy mission from Harbour city towards Moelville across route-005, as presented in Figure 10.2, with three distinct episodes that map to the aforementioned functionalities, namely:

1. Mission preparation (i, ii, iii, iv)
2. Transition from AoO-1 to AoO-2 (v, vi, vii)
3. Enemy detection/engagement (viii, ix)

Figure 10.2: Visualization of presented scenario.

10.4 Validation Episodes

10.4.1 Episode 1: Mission preparation

The mission preparation stage for a given tactical operation requires the deployment of the corresponding pre-defined security policies and the services that constitute the security architecture (both core and functional). The syntactical and procedural methods for the development of the security policy framework have been presented in detail at [11, 8, 10], while the requirements, functionalities and interactions of the security services within the TACTICS TSI [5] have been presented at [14, 13]. Furthermore, the policy distribution method for the mission preparation stage has been described at [12].

10.4.1.1 i. Capturing and incorporation of fine-grained network semantics of static and dynamic nature across the security policy:

The examined scenario requires the incorporation of the elements presented in Figure 10.3 within the security policy. As described in the aforementioned studies, this is achieved with the use of unary (concept assertions) and binary (role assertions) predicates within an ontologically constructed knowledge-base. This allows capturing refined attributes of the involved entities (services, information, networks, radios, nodes, and subjects), and defining fine-grained interactions among them. Furthermore, the use of Terminology/ Assertion/ Rule triplets allows the definition of additional constraints such as separation of duty, although such declarations increase the complexity.

It must be noted that due to their multitude, the information elements of this scenario have not been listed in Figure 10.3 (only the three core subcategories). Yet the Information policy branch can be used to demonstrate the expressive power of the developed mechanism. As an example, the 'Picture functional service' can generate three different image formats (namely PNG, JPG, and BMP), which serve distinct purposes (e.g. can be utilised by other services, such as being incorporated in a MEDEVAC request), and have distinct attributes and security restrictions (e.g. access control, compression preferences, and priority). Each of the formats is defined as an individual within the Information/ SystemSpecific subclass (see Figure 10.4). This allows the definition of fine-grained data properties, that can be identified as functional (unique) and with constrained ranges. Furthermore, relationships between individual are defined with the use of object properties, which can be constrained in range but also identified as Functional, Inverse functional, Transitive, Symmetric, Asymmetric, Reflexive or Irreflexive.

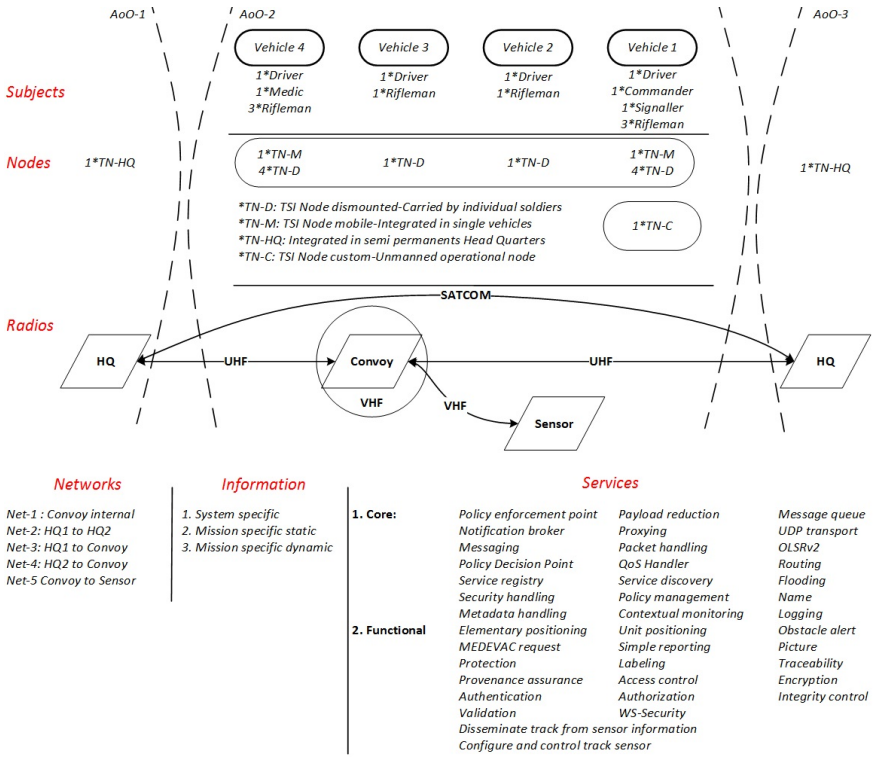

Figure 10.3: Security policy components for the examined scenario.

Focusing on specific aspects of this example, the source of each information element has been constrained to individuals that belong to the subjects, services, and nodes classes, by defining the appropriate ranges and domains. Additionally, functional object properties have been used to establish direct links for the given individuals. As an example, the unique source of the 'PictureServiceOutputJPG' is defined to be the 'PictureService' individual as:

```
<owl:ObjectProperty rdf:ID="InformationHasSourceService">
<rdf:type rdf:resource="&owl;FunctionalProperty" />
<rdfs:domain rdf:resource="Information" />
<rdfs:range rdf:resource="Service" />
</owl:ObjectProperty>

<owl:NamedIndividual rdf:about="PictureServiceOutputJPG">
<Episode1-Policy:InformationHasSourceService rdf:resource="#
    ↪ PictureService"/>
```

Similar declarations are established in order to denote all the relationships across the mission components, such as subjects using a specific node, nodes participating in networks, services being deployed on nodes, and radios serving specific networks.

```
<owl:NamedIndividual rdf:about="http://.../Episode1-Policy#PictureServiceOutputJPG">
<rdf:type rdf:resource="http://.../Episode1-Policy#SystemSpecific"/>
<Episode1-Policy:CanDelete rdf:resource="http://.../Episode1-Policy#PictureService"/>
<Episode1-Policy:HasFullControl rdf:resource="http://.../Episode1-Policy#PictureService"/>
<Episode1-Policy:HasOwner rdf:resource="http://.../Episode1-Policy#PictureService"/>
<Episode1-Policy:HasBitDepth rdf:datatype="http://.../XMLSchema#integer">24</Episode1-Policy:HasBitDepth>
<Episode1-Policy:HasEncodingFormat rdf:datatype="http://.../XMLSchema#string">jpeg</Episode1-Policy:HasEncodingFormat>
<Episode1-Policy:HasHeight rdf:datatype="http://.../XMLSchema#integer">996</untitled-ontology-87:HasHeight>
<Episode1-Policy:HasHorizontalResolution rdf:datatype="http://.../XMLSchema#integer">120</Episode1-Policy:HasHorizontalResolution>
<Episode1-Policy:HasImageIDRangeHigh rdf:datatype="http://.../XMLSchema#integer">2750</Episode1-Policy:HasImageIDRangeHigh>
<Episode1-Policy:HasImageIDRangeLow rdf:datatype="http://.../XMLSchema#integer">1750</Episode1-Policy:HasImageIDRangeLow>
<Episode1-Policy:HasSize rdf:datatype="http://.../XMLSchema#integer">267000</Episode1-Policy:HasSize>
<Episode1-Policy:HasTittle rdf:datatype="http://.../XMLSchema#string">PictureServiceOutput</Episode1-Policy:HasTittle>
<Episode1-Policy:HasVerticalResolution rdf:datatype="http://.../XMLSchema#integer">120</Episode1-Policy:HasVerticalResolution>
<Episode1-Policy:HasWidth rdf:datatype="http://.../XMLSchema#integer">1154</Episode1-Policy:HasWidth>
</owl:NamedIndividual>
```

Figure 10.4: Partial policy fragment for 'PictureServiceOutputJPG' information/individual.

10.4.1.2 ii. Fine-grained action governance/definition, according to the developed (Domain $\longmapsto$ Capability $\longmapsto$ Action) paradigm:

The formal policy model presented in [11], describes in detail the notions of Domain, Capability and Action, as well as how these elements are defined and utilised for the enforcement of security controls across the elements and activities of a tactical operation.

In short, the TACTICS capabilities have been defined in accordance to the NATO Capability View [23], while in the context of the security policy have been extended to include all interactions across the components of a given tactical operation. Examples of the defined capabilities are "Effects management", "Shared situational awareness", "Fire support", "Tasking and Ordering", and "Force protection". Furthermore, the security domains have been defined as a result of the analysis for system specific requirements, initiated in [8] and presented in detail at [10] and [14]. These domains facilitate the enforcement of the protection goals established in the aforementioned studies, and include Planning, Protection, Detection, Diligence and Response. Finally, the mission specific actions correspond to the intersection of domains and capabilities, establishing the framework for the enforcement of security controls across the capabilities required for a tactical operation.

Therefore policy decision requests are formulated across TACTICS TSI in the form of action governance, that need to be resolved by the security architecture. The Domain $\longmapsto$ Capability $\longmapsto$ Action paradigm, has been integrated as a functionality of the developed 'Security Handling service', in the form of a distinct knowledge-base.

For the "PictureServiceOutput", the protection domain includes elements such as encryption, integrity, labelling and access control. Using encryption as an example, the actions of enforcing specific algorithms through the 'Encryption' functional service are defined as:

```
Declaration(Class(:Domain))
Declaration(Class(:Protection))
# Class: :Protection (:Protection)
SubClassOf(:Protection :Domain)

Declaration(Class(:Capability))
Declaration(Class(:PictureServiceOutput))
# Class: :PictureServiceOutput (:PictureServiceOutput)
SubClassOf(:PictureServiceOutput :Capability)

Declaration(Class(:Action))
Declaration(Class(:EncryptionPictureServiceOutputJPG))
# Class: :EncryptionPictureServiceOutputJPG (:
    ↪ EncryptionPictureServiceOutputJPG)
SubClassOf(:EncryptionPictureServiceOutputJPG :Action)

Declaration(ObjectProperty(:HasEnforcementMechanism))
Declaration(DataProperty(:HasCapability))
Declaration(DataProperty(:HasDomain))
Declaration(NamedIndividual(:NoEncryption))
Declaration(NamedIndividual(:Alg1TDES))
Declaration(NamedIndividual(:Alg2128AES))
Declaration(NamedIndividual(:Alg3256AES))
Declaration(NamedIndividual(:EncryptionFService))

# Individual: :Alg1TDES (:Alg1TDES) %Similarly for:
    ↪ Alg2128AES, Alg3256AES, and NoEncryption
ClassAssertion(:EncryptionPictureServiceOutputJPG :Alg1TDES)
ObjectPropertyAssertion(:HasEnforcementMechanism :Alg1TDES :
    ↪ EncryptionFService)
DataPropertyAssertion(:HasCapability :Alg1TDES "
    ↪ PictureServiceOutput"^^xsd:string)
DataPropertyAssertion(:HasDomain :Alg1TDES "Protection"^^xsd:
    ↪ string)
DataPropertyAssertion(:HasPriority :Alg1TDES 2)
```

It must be noted that actions can be defined as referring to singular entities to enhance granularity (e.g 'EncryptionPictureServiceOutputJPG' as presented in this example), or be grouped in order to improve reasoning efficiency. As an example, this would allow to enforce the same subset of integrity protection mechanisms, to all text files generated using the Messaging functional service from specific nodes, by subjects with rank higher or

equal to captain. Implementing, such grouping requires only the declaration of appropriate object and data properties and the definition of constrained subclasses under the "Capability" class. Constrained subclasses are defined by restricting the instances of the subclass according to constrained values of object and data properties.

10.4.1.3 iii. Definition of prioritised rule set per action according to the developed paradigm:

Governance for the defined actions within the security policy, as presented in the two previous paragraphs, is established by creating links between the actions and the security policy knowledge base. This is achieved by the integration of a prioritised rule set per action, which incorporates constrained values for specific object and data properties, as presented in detail at [11]. The definition and distribution of these rule sets is executed at the strategic domain, during the mission preparation stage.

Furthermore, this process allows the on-line policy adaptation to dynamic network semantics, by the definition of corresponding rules. This feature has been demonstrated by extending the previous example, towards the selection of the encryption algorithm to be used for the transmission of a message by the "Simple reporting" functional service. This test-case refers to the Domain: Protection, Grouped Capability: SimpleReporting _MessageType265, and Action: Encryption-SimpleReporting _MessageType-265, with available instances being Alg1TDES, Alg2128AES, and NoEncryption. For the selection of the algorithm any combination of object and data properties can be evaluated, while in this test-case it was defined in accordance to the current network capacity (Net-3: HQ1 to Convoy), message classification, and message precedence, as:

```
Rule 1:Has_Current_Capacity(Net3,"Medium"),
    ↪ Has_Classification(MessageType265,?x), swrlb:lessThan(?
    ↪ x,4) -> Encrypt(Alg1TDES,MessageType265)

Rule 2:Has_Current_Capacity(Net3,"Low") -> Encrypt(Alg1TDES,
    ↪ MessageType265)

Rule 3:Has_Current_Capacity(Net3,"Low"), Has_Precedence(
    ↪ MessageType265,"FlashOverride") -> Encrypt(NoEncryption
    ↪ ,MessageType265)
```

In this episode the generic rule established within the security policy, requires the use of 'Alg2128AES' for the encryption of messages that are instances of the MessageType265 class. Yet, rule 1 allows the use of 'Alg1TDES' when the network capacity is 'Medium', and the message classification is less than '4'. Furthermore, rule 2 also allows the use of 'Alg1TDES', when

the network capacity is 'Low', regardless of message classification or precedence. Finally, when the network capacity is 'Low', and the message precedence is 'Flash Override', rule 3 allows the use of 'NoEncryption', in order to accommodate life preservation alerts. The extraction of these instances within the security service architecture, is achieved by querying the 'Metadata handling service' in respect to the examined action. Such queries may have high complexity, incorporating additional rules (as defined and retrieved from the 'Policy Decision Point' service), or as in this example be only restricted by the examined domain and capability, such as:

```
SELECT ?instance
WHERE {?instance:Has_Domain "Protection"^^xsd:string ;
       :Has_Capability "SimpleReporting_MessageType265"^^xsd:
           ↪ string ;
       :Has_Priority 1}
```

Similarly, on-line policy adaptation can be enforced in all aspects referring to interactions among the components of a tactical operation, accommodating scenarios of increased complexity as presented in the following episodes.

10.4.1.4 iv. Scalability of policy and service infrastructure:

The notion of scalability from the perspective of security within TACTICS, refers primarily to the capacity of deploying security controls (e.g. Policies and services) across the four described types of nodes (TN-D, TN-M, TN-HQ, and TN-C: see Figure 10.3), maintaining operability.

In respect to the security policy framework, a detailed analysis of the constrains involved in its distribution, has been presented at [12]. The same article presents a suitable mechanism for the optimization of partitioning and distributing security policy fragments, across the various types of deployed nodes during the mission preparation stage. Yet, the incorporation of dynamic semantics and the aforementioned capability for on-line policy adaptation, will induce divergences across the local policies during the tactical operation. The executed scenarios allowed us to identify the nature of these divergences, and develop a mechanism for their reconciliation optimized for the examined tactical SOA, as presented in [9].

From the perspective of services, the developed core architecture, comprising of six services and presented in [13], is required to be deployed across all the involved nodes, in order to support the functionalities of the security policy framework. Nevertheless, the use of semantic web technologies facilitate additional flexibility both at the implementation and operational phases, by allowing the selective utilization of inference subsystems. Within TACTICS, for experimental and demonstration purposes, Apache-Jena has been used for the development of the 'Metadata handling' core service, where the reasoning and extraction of policy decisions occurs. Apache-

Jena [31] allows a range of inference engines (RSDF, Micro, Mini, Full) to be integrated across the tactical nodes, according to the complexity and requirements of the deployed policy fragment after distribution. The fragment of the code implementing this functionality over the two non-constrained types of nodes (TN-HQ, TN-M), is:

```
package eu.tacticsproject.service.metadatahandling.reasoner;
import org.apache.jena.rdf.model.InfModel;
import org.apache.jena.rdf.model.Model;
import org.apache.jena.reasoner.Reasoner;
import javax.jws.WebMethod;
import javax.jws.WebService;
import javax.jws.soap.SOAPBinding;
import javax.jws.soap.SOAPBinding.Style;

public interface InferenceEngine {
  Model loadPolicy(String file, String type);
  Model loadInstance(String file, String type);
  Reasoner getJenaReasoner(String reasonerType);
  Reasoner createReasoner (Model tbox, String type);
  InfModel createModel(Reasoner reasoner, Model abox);}
```

```
package eu.tacticsproject.service.metadatahandling.reasoner;
import org.apache.jena.rdf.model.InfModel;
import org.apache.jena.rdf.model.Model;
import org.apache.jena.rdf.model.ModelFactory;
import org.apache.jena.reasoner.Reasoner;
import org.apache.jena.reasoner.ReasonerRegistry;
import org.apache.jena.reasoner.ValidityReport;
import org.apache.jena.util.FileManager;
import org.springframework.stereotype.Service;

@Service
public class InferenceEngineImpl implements InferenceEngine {
@Override
public Model loadPolicy(String file, String type)
  {return FileManager.get().loadModel(file, null, type);}
@Override
public Model loadInstance(String file, String type)
  {return FileManager.get().loadModel(file, null, type);}
@Override
public Reasoner getJenaReasoner(String reasonerType) {
  if("RSDF".equalsIgnoreCase(reasonerType))
  {return ReasonerRegistry.getRDFSReasoner();}
  else if("Micro".equalsIgnoreCase(reasonerType))
  {return ReasonerRegistry.getOWLMicroReasoner();}
  else if("Mini".equalsIgnoreCase(reasonerType))
```

```
  {return ReasonerRegistry.getOWLMiniReasoner();}
  else if("Full".equalsIgnoreCase(reasonerType))
  {return ReasonerRegistry.getOWLReasoner();}
  return null;}
@Override
public Reasoner createReasoner(Model tbox, String type)
  {return getJenaReasoner(type).bindSchema(tbox.getGraph());}
@Override
public InfModel createModel(Reasoner reasoner, Model abox)
  {return ModelFactory.createInfModel(reasoner, abox);}
@Override
public boolean isValid(InfModel infModel)
  {ValidityReport report = infModel.validate();
return report.isValid();}}
```

Furthermore, the defined functional services are deployed across the tactical nodes, according to their operational requirements. As an example, the 'MEDEVAC request' functional service is deployed in the examined scenario at the nodes TN-M:Vehicle 4, TN-D (medic):Vehicle 4, and TN-M:Vehicle 1 for redundancy but with on-line adaptation constraints. Accordingly, the corresponding policy fragment, governing interactions between this service and other component (Services, Information, Networks, Radios, Nodes, and subjects) is distributed as described in the aforementioned studies.

10.4.2 Episode 2

In this episode the convoy transitions from AoO-1 into AoO-2 at point 2*, as presented in Figure 10.2. The convoy is connected to the Head-Quarters through two UHF networks, namely Net-3 (HQ1 to convoy) and Net-4 (HQ2 to convoy). Furthermore, a custom TSI node becomes available (TN-C: Sensor), through a VHF network (Net-5: Convoy to Sensor).

10.4.2.1 v. Adaptability to rapid network alterations:

The capacity of the security architecture to adapt to network alterations, has been demonstrated earlier in respect to the encryption algorithm selection for MessageType265. Yet this episode has been developed in order to highlight the details of the process and provide additional examples.

The individuals from the networks and nodes policy fragments are presented in Figure 10.5, in accordance to the requirements of the examined scenario. Defining the data properties of individuals as presented in Episode 1, accommodates the security policy reasoning and adaptation to mission dynamics, such as adapting security decisions to network quality metrics or node resource availability.

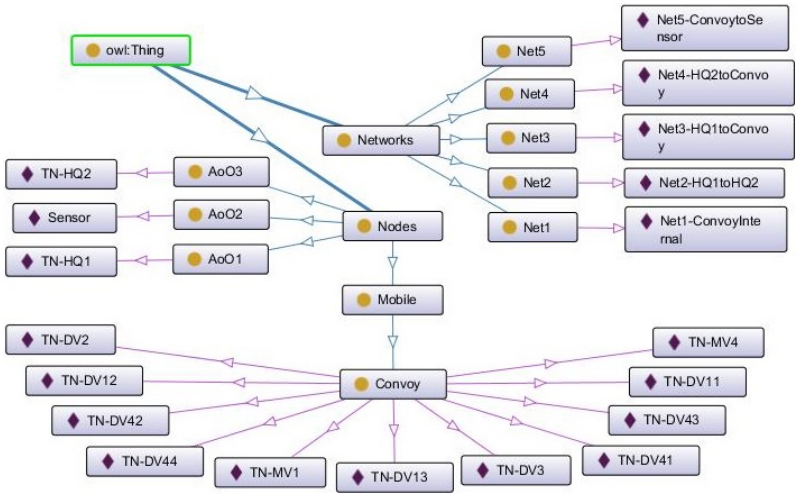

Figure 10.5: Individuals for the networks and nodes policy fragments.

Furthermore, this example can illustrate the use of object properties for the establishment of relationships between individuals. As an example, the nodes served by Net1-ConvoyInternal are defined with the use of two inverse object properties (HasHosts, IsHostInNetwork), establishing the relationships presented in Figure 10.6.

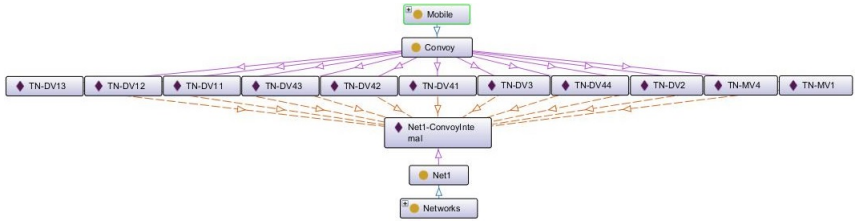

Figure 10.6: Definition of nodes served by Net1-ConvoyInternal.

10.4.2.2 vi. Ability to substitute actions on-line:

Additionally to adapting policy decisions according to timely values of entity data properties, on-line action substitution is also possible. Continuing the example of the previous paragraph, the examined test-case refers to the dissemination of blue force tracking data from the convoy towards the Head-Quarters with the use of of the Unit positioning functional service. The deployed TN-MV1 node (the capability is also deployed to TN-MV2 for

redundancy) collects the data and periodically transmits them as a bundle towards one of the two Head-quarters (TN-HQ1, TN-HQ2). This information instance is defined as EXTBFT_Update, with data properties that include "Classification: 10" and "Precedence: Routine". Therefore this example refers to Domain: Diligence, Capability: SharedSituationalAwareness, and ActionSet: Disseminate_EXTBFT_Update. The diligence domain incorporates specific security requirements for each action (e.g. encryption, integrity, provenance assurance), while out of the available actions the most suitable is identified in order to accommodate these requirements according to the currently available resources. For the examined test-case four action options must be under policy governance, defined as:

- **Action 1:** Transmit to TN-HQ1 through Net-3. (if Net-3 can support the security overhead)
- **Action 2:** Transmit to TN-HQ2 through Net-4. (if Net-4 can support the security overhead)
- **Action 3:** Store locally and attempt later (if neither Net-3 nor Net-4 can support the security overhead, and the required resources are available in the Message queue core service.)
- **Action 4:** Drop the bundle. (if none of the aforementioned conditions apply.)

This decision carries implications that relate both to security (e.g. channel utilization equalization protection goal) and QoS (Quality of Service), while the interoperability mechanism between the two has been presented earlier [34]. Across AoO-2 continuous connectivity is not maintained towards neither of the Head-Quarters. In order to simplify the example the underlying technical details (e.g throughput, packet error rate, encryption overhead, integrity protection overhead, latency) have been omitted, although such a policy decision can be defined according to fine-grained semantics as presented earlier. Accordingly, the selection of the appropriate action relies on aggregated semantics, such as each networks' capacity to support the load of secure transmission (denoted as: SupportSecLvL), and the available local node resources (denoted as: PacketHandlerBufferLvL). Therefore the governance of the required actions is achieved by defining corresponding rules, as:

```
Rule 1 (For Action 1): SupportSecLvL(Net3–HQ1toConvoy, ?x),
    ↪ swrlb:greaterThan(?x, 8) –> DisseminateEXTBFT_Update(TN
    ↪ –HQ1, EXTBFT_Update)

Rule 2 (For Action 2): SupportSecLvL(Net4–HQ2toConvoy, ?x),
    ↪ swrlb:greaterThan(?x, 8) –> DisseminateEXTBFT_Update(TN
    ↪ –HQ2, EXTBFT_Update)
```

```
Rule 3 (For Action 3): PacketHandlerBufferLvL(TN-MV1, ?x),
    ↪ swrlb:greaterThan(?x, 5), SupportSecLvL(Net4-
    ↪ HQ2toConvoy, ?y), SupportSecLvL(Net3-HQ1toConvoy, ?y),
    ↪ swrlb:lessThan(?y, 8) -> DisseminateEXTBFT_Update(
    ↪ StoreEXTBFT_Update-MQS, EXTBFT_Update)

Rule 4 (For Action 4): PacketHandlerBufferLvL(TN-MV1, ?x),
    ↪ swrlb:lessThanOrEqual(?x, 5), SupportSecLvL(Net4-
    ↪ HQ2toConvoy, ?y), SupportSecLvL(Net3-HQ1toConvoy, ?y),
    ↪ swrlb:lessThan(?y, 8) -> DisseminateEXTBFT_Update(
    ↪ Drop_EXTBFT_Update, EXTBFT_Update)
```

10.4.2.3 vii. Standalone node operation:

According to the TACTICS requirements, nodes that have been deployed as standalone, or have lost connectivity with a mission network, must have an explicit policy and service infrastructure in place, in order to handle prolonged isolation and maintain operability. Accordingly, the minimum set of core services deployed in a tactical node must allow service discovery, message exchange and security. Therefore, the deployed sensor (node: TN-C, Figure 10.3) must incorporate the required policies, along with the functional and core services that would allow the dissemination of tracks, as required by the scenario.

Focusing on security, this is mapped to the notions presented across this article and the inherent modularity of SOA. Therefore, the sensor would have to support the six core security services, with the following adaptations:

1. Security Handling service:
   - Implementation of the fragment that refers only to the supported Domains, Capabilities and Actions. (see paragraph 10.4.1.2)
   - Increased incorporation of pre-computed policy decisions. (see paragraph 10.4.3.2)
2. Policy Management service: No viable adaptation.
3. Policy Decision Point service: (see paragraph 10.4.1.3)
   - Incorporation of the rules that refer only to the supported actions.
   - Prioritization of rules with reduced complexity.
4. Metadata Handling service:

- Implementation of the knowledge-base fragment that refers only to the supported actions and deployed limited rule set. (see paragraph 10.4.1.1)
- Integration of low complexity inference engines. (See paragraph 10.4.1.4)

5. Contextual Monitoring service:
   - Capturing and statistical analysis of limited sub-set of dynamic semantics, according to the requirements of the 'Metadata Handling' knowledge-base fragment.
6. Policy Enforcement Point service:
   - Integration of interfaces only towards the deployed functional services.

10.4.3 Episode 3

In this episode the convoy reaches point 3* in Figure 10.2, where it is attacked by a small group of insurgents. Two of the test-cases from this episode are presented, in order to highlight additional functionalities of the security architecture.

10.4.3.1 viii. Ability to transition between governing rules, and fall back operation:

As presented in the previous paragraphs, policy decision requests are formulated within TACTICS TSI in the form of action governance, which correspond to the enforcement of security controls (domains) across the deployed Capabilities. This is achieved by the definition of a prioritized rule set of increased complexity for each action, by incorporating static and dynamic system semantics in order to support fine-grained and adaptable security enforcement.

Fragments of each rule set are deployed across the nodes according to the computational capacity of each node, while the prioritization of the rules is based on their complexity. As mentioned in paragraph 10.4.1.4, the 'MEDEVAC request' functional service is deployed at the nodes TN-M:Vehicle 4, TN-D(Medic):Vehicle 4, and TN-M:Vehicle 1. For the Domain:Protection, Capability: ForceProtection, and Action: AccessControlTACTICSMEDEVAC, the following prioritized rule set (presented in Manchester syntax) can be used in order to illustrate the expressive capacity of such rules.

1. 1st priority rule:

```
Node_SupportsService value "TacticsMEDEVAC"
Node_hasSubject some AllSubjects
(Subject_hasTrustLevel value "High") and ((
    ↪ Node_hasTrustLevel value "High") or (
    ↪ Node_hasTrustLevel value "Medium"))
(Node_hasAoO value "AoO2") or (Node_hasAoO value "AoO3")
(Subject_hasRank value "CPT") or (Subject_hasRank value "
    ↪ LTA") or (Subject_hasRank value "2LT") or (
    ↪ Subject_hasFunction value "MEDIC")
Node_hasMissionType value "Convoy"
((Node_hasOperationalGroup value "G2") and (Node_hasType
    ↪ value "TSI_ND")) or ((Node_hasOperationalGroup
    ↪ value "G1") and (Node_hasType value "TSI_NM"))
(Node_hasSupportRadioITUDesignation value "UHF") or (
    ↪ Node_hasSupportRadioITUDesignation value "VHF")
Node_hasSupportProtocol value "TLS/ SSH"
```

2. 2nd priority rule:

```
Node_SupportsService value "TacticsMEDEVAC"
Node_hasSubject some AllSubjects
(Subject_hasTrustLevel value "High") and ((
    ↪ Node_hasTrustLevel value "High") or (
    ↪ Node_hasTrustLevel value "Medium"))
(Subject_hasRank value "CPT") or (Subject_hasRank value "
    ↪ LTA") or (Subject_hasRank value "2LT") or (
    ↪ Subject_hasFunction value "MEDIC")
Node_hasMissionType value "Convoy"
(Node_hasOperationalGroup value "G2") or ((
    ↪ Node_hasOperationalGroup value "G1")
(Node_hasSupportRadioITUDesignation value "UHF") or (
    ↪ Node_hasSupportRadioITUDesignation value "VHF")
Node\_hasSupportProtocol value "TLS/ SSH"
```

3. 3rd priority rule:

```
Node_SupportsService value "TacticsMEDEVAC"
Node_hasSubject some AllSubjects
(Subject_hasTrustLevel value "High") and ((
    ↪ Node_hasTrustLevel value "High") or (
    ↪ Node_hasTrustLevel value "Medium"))
(Subject_hasRank value "Medium") or (Subject_hasFunction
    ↪ value "MEDIC")
```

```
Node_hasMissionType value "Convoy"
(Node_hasOperationalGroup value "G2") or ((
    ↪ Node_hasOperationalGroup value "G1")
Node_hasSupportProtocol value "TLS/ SSH"
```

The selection of a rule for the resolution of an action request is done by the 'Policy Management' service, and depends on the available node resources at the time of the request. The resource indicator is contained in the 'securityDecisionRequest', while the identifier of the selected rule is denoted as 'actionIDCyclesToLive()':

```
package eu.tacticsproject.service.policymanagement;
@Service
public class PolicyManagementService {
@Autowired
private ActionRequestRepository actionRequestRepository;
@Autowired
private PolicyDecisionPointService policyDecisionPointService
    ↪ ;
public SecurityDecision getSecurityDecision(
    ↪ SecurityDecisionRequest securityDecisionRequest) {
actionRequestRepository.save(securityDecisionRequest.
    ↪ getActionRequestId());
ActionRequest_IDBundle actionRequestIdBundle =
    ↪ ActionRequest_IDBundle.builder()
.actionRequestId(securityDecisionRequest.getActionRequestId()
    ↪ )
.refreshAlert(securityDecisionRequest.isRefreshAlert())
.actionIDCyclesToLive() ← Rule identifier
.build();
SecurityDecision securityDecision =
    ↪ policyDecisionPointService.getSecurityDecision(
    ↪ actionRequestIdBundle);
return securityDecision;}
```

Consequently, as presented in the code extract, the constructed 'ActionRequest _IDBundle' is send to the 'Policy Decision Point' service, where the requested rule is extracted and send for reasoning at the 'Metadata Handling' service.

10.4.3.2 ix. Incorporation of pre-computed policy decisions:

As presented earlier, under highly congested or disrupted environments, functionality is maintained by the use of policy fragments and rules with decreased complexity. Furthermore, the 'Security Handling' service is the first core security service that process an action request towards the extraction of a policy decision. Along with the various adaptation functionalities,

the 'Security Handling' service has been defined and developed with the capacity to accommodate pre-computed policy decisions. This, has been dictated by the requirement to maintain a minimum of service functionality, under any operable conditions.

Therefore, at the mission preparation stage a statistical analysis can provide a subset of action requests with increased frequency, or high criticality. For such action requests, pre-computed policy decisions are established in the form of access control lists. Such policy decisions are utilised only within a constrained range of conditions, yet allow the enforcement of security controls with the invocation of a minimum set of services and without initiating the reasoning process. As presented in the following code fragment from the TACTICS TSI implementation, each "actionRequest" is mapped to a uniquely identified "actionRequestId", which is evaluated from the "getPreComputedPolicyDecision" function. This function evaluates the existence of a pre-computed policy decision for the given "actionRequest" and calls for the timely values of a limited set of semantics from the 'Contextual Monitoring' service. If these are within the range for which the pre-computed policy decision is valid, then the decision is send directly to the 'Policy Enforcement Point' service. Otherwise, the decision extraction process continues towards the 'Policy Management' service.

```
package eu.tacticsproject.service.securityhandling;
@Service
public class SecurityHandlingService {
@Autowired
private ContextualMonitoringService
    ↪ contextualMonitoringService;
@Autowired
private PolicyEnforcementPointService
    ↪ policyEnforcementPointService;
@Autowired
private PolicyManagementService policyManagementService;

public ActionResponse send(ActionRequest actionRequest) {
ActionRequestId actionRequestId = generateActionRequestId(
    ↪ actionRequest);
String policyDecision = getPreComputedPolicyDecision(
    ↪ actionRequestId);
AttributeValuesRequest attributeValuesRequest =
    ↪ generateAttributeValuesRequest();
AttributeValuesResponse attributeValues =
    ↪ contextualMonitoringService.getAttributeValues(
    ↪ attributeValuesRequest);

if (getPreComputedPolicyDecision(actionRequestId) != null) {
SecurityDecision securityDecision = generateSecurityDecision(
```

```
    ↪ actionRequestId);
return policyEnforcementPointService.getActionResponse(
    ↪ securityDecision);}
else { ... }}
```

10.5 Conclusions

The project TACTICS was undertaken in order to provide a proof of concept for the capacity to deploy the required capabilities at the tactical edge, and develop a service infrastructure tailored to the requirements of the modern battlefield. In this article, a comprehensive view of the developed security framework is presented, according to the scenarios executed during the concluding system validation demonstrations. A subset of the security related functionalities supported by the developed TACTICS TSI have been presented, highlighting critical architectural details towards its implementation. Furthermore, this article unifies the publicly available results of our security related studies, by highlighting how the distinct components presented earlier, interoperate towards the enforcement of security controls within tactical SOA. The presented results, highlight the capacity of tactical networks to support efficient security controls, given that the corresponding requirements and constraints are satisfied.

Through the executed studies across TACTICS, and after its successful completion, a variety of future work paths have been identified. These include the investigation of integrated QoS and Security policies particularly for networks with volatile connectivity or link quality, and trust models for store-and-forward bundling, particularly in coalition environments. Furthermore, another potentially critical path of future work, refers to the investigation of efficient service and message delivery mechanisms for transitions between different levels of connectivity, down to outright disruption.

Acknowledgments

The results described in this work were obtained as part of the European Defence Agency project TACTICS (Tactical Service Oriented Architecture). The TACTICS project is jointly undertaken by Patria (FI), Thales Communications & Security (FR), Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE (DE), Thales Deutschland (DE), Leonardo (IT), Thales Italia (IT), Norwegian University of Science and Technology (NO), ITTI (PL), Military Communication Institute (PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980.

Bibliography

[1] ALOISIO, A., AUTILI, M., D'ANGELO, A., VIIDANOJA, A., LEGUAY, J., GINZLER, T., LAMPE, T., SPAGNOLO, L., WOLTHUSEN, S. D., FLIZIKOWSKI, A., AND SLIWA, J. TACTICS: TACTICal Service Oriented Architecture. *CoRR abs/1504.07578* (2015). Available from: `http://arxiv.org/abs/1504.07578`. 43, 63, 103, 121, 143, 154, 189, 191, 212

[2] BARTOLOMASI, P., BUCKMAN, T., CAMPBELL, A., GRAINGER, J., MAHAFFEY, J., MARCHAND, R., KRUIDHOF, O., SHAWCROSS, C., AND VEUM, K. Nato network enabled capability feasibility study. *Version 2.0* (2005). 212

[3] BLOEBAUM, T. H., AND LUND, K. Consis: Demonstration of soa interoperability in heterogeneous tactical networks. In *2012 Military Communications and Information Systems Conference (MCC)* (Oct 2012), pp. 1–7. 214

[4] DAMIANOU, N., DULAY, N., LUPU, E., AND SLOMAN, M. The ponder policy specification language. *Policy 1* (2001), 18–38. 18, 19, 84, 143, 165, 215

[5] DIEFENBACH, A., GINZLER, T., MCLAUGHLIN, S., SLIWA, J., LAMPE, T. A., AND PRASSE, C. Tactics tsi architecture: A european reference architecture for tactical soa. In *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (May 2016), pp. 1–8. 63, 103, 121, 144, 155, 218

[6] EDA. NEC implementation study final report, EDA 08-CAP-19, 2010. 212

[7] FERRINI, R., AND BERTINO, E. Supporting RBAC with XACML + OWL. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT '09)* (Stresa, Italy, June 2009), B. Carminati and J. Joshi, Eds., ACM Press, pp. 145–154. 84, 165, 214

[8] GKIOULOS, V., AND WOLTHUSEN, S. D. Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Net-

works. *Norwegian Information Security Conference - NISK* (2015), 109–120. 43, 63, 103, 113, 122, 123, 143, 166, 168, 189, 191, 213, 218, 220

[9] GKIOULOS, V., AND WOLTHUSEN, S. D. Efficient security policy reconciliation in tactical service oriented architectures. In *International Conference on Future Network Systems and Security* (2016), Springer, pp. 47–61. 43, 63, 103, 113, 122, 123, 213, 223

[10] GKIOULOS, V., AND WOLTHUSEN, S. D. Securing tactical service oriented architectures. In *2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)* (July 2016), pp. 1–6. 63, 71, 103, 113, 122, 123, 143, 154, 157, 189, 191, 213, 218, 220

[11] GKIOULOS, V., AND WOLTHUSEN, S. D. A security policy infrastructure for tactical service oriented architectures. In *Conference on Security of Industrial-Control-and Cyber-Physical Systems* (2016), Springer, pp. 37–51. 63, 103, 104, 113, 122, 123, 213, 218, 220, 222

[12] GKIOULOS, V., AND WOLTHUSEN, S. D. *Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures*. Springer International Publishing, Cham, 2017, pp. 149–166. Available from: `http://dx.doi.org/10.1007/978-3-319-44354-6_9`. 43, 63, 103, 113, 114, 122, 123, 143, 189, 191, 213, 218, 223

[13] GKIOULOS, V., AND WOLTHUSEN, S. D. Security infrastructure for service oriented architectures at the tactical edge. 310–322. 214, 218, 223

[14] GKIOULOS, V., AND WOLTHUSEN, S. D. Security Requirements for the Deployment of Services Across Tactical SOA. *7th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security* (2017). 103, 213, 218, 220

[15] HELIL, N., AND RAHMAN, K. Extending xacml profile for rbac with semantic concepts. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on* (Oct 2010), vol. 10, pp. V10–69–V10–74. 84, 165, 214

[16] JOHNSEN, F., BLOEBAUM, T., SCHENKELS, L., FISKE, R., VAN SELM, M., DE SORTIS, V., VAN DER ZANDEN, A., SLIWA, J., AND CABAN, P. SOA over disadvantaged grids experiment and demonstrator. In *Communications and Information Systems Conference (MCC), 2012 Military* (Oct 2012), pp. 1–8. 42, 83, 165, 214

[17] MALOWIDZKI, M., DALECKI, T., BEREZINSKI, P., MAZUR, M., AND SKARZYNSKI, P. Adapting standard tactical applications for a military disruption-tolerant network. In *2016 International Conference on Military*

Communications and Information Systems (ICMCIS) (May 2016), pp. 1–5. 15, 214

[18] MANSO, M., CALERO, J. M. A., BARZ, C., BLOEBAUM, T. H., CHAN, K., JANSEN, N., JOHNSEN, F. T., MARKARIAN, G., MEILER, P.-P., OWENS, I., ET AL. Soa and wireless mobile networks in the tactical domain: Results from experiments. In *Military Communications Conference, MILCOM 2015-2015 IEEE* (2015), IEEE, pp. 593–598. 121, 214

[19] NATO. NATO Architecture Framework (NAF) version 3.0, 2007. 212

[20] NATO. NATO Network Enabled Capability Feasibility Study Volume I: NATO Network-Centric Operational Needs And Implications For The Development Of Net-Centric Solutions, version 2.0, 2005. 212

[21] NATO. NATO Network Enabled Feasibility Study Volume II: Detailed Report Covering a Strategy and Roadmap for Realizing an NNEC Networking and Information Infrastructure, version 2.0, 2005. 212

[22] NATO ALLIED COMMAND TRANSFORMATION. NATO Network-Enabled Capability (NNEC) Vision & Concept, 2006. 212

[23] NATO CONSULTATION, COMMAND AND CONTROL BOARD BOARD (NC3B). C3 Taxonomy Perspective, Baseline 2.0, Enclosure 2 to 6300 TSC FCX 0010/TT-151521/Ser:NU, NC3B, November 2015. 43, 214, 220

[24] NONES, M., AND MARRONE, A. The Transformation of the Armed Forces: The Forza NEC Program. *Roma, Nuova Cultura,174 p.* (2012). 214

[25] OASIS. Oasis security services (saml) tc. Available from: `https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security`. 84, 143, 165, 214

[26] OASIS STANDARD SPECIFICATION: WEB SERVICE SECURITY (WSS) TECHNICAL COMMITTEE. Web Services Security: SOAP Message Security 1.1, February 2006. 215

[27] RAMLI, C. D. P. K., NIELSON, H. R., AND NIELSON, F. The Logic of XACML. *Science of Computer Programming 83* (Apr. 2014), 80–105. 84, 143, 165, 214

[28] SEIFERT, H., FRANKE, M., DIEFENBACH, A., AND SEVENICH, P. SOA in the CoNSIS coalition environment: Extending the WS-I Basic Profile for using SOA in a tactical environment. In *2012 Military Communications and Information Systems Conference (MCC)* (Oct 2012), pp. 1–6. 17, 214

[29] SLIWA, J., AND JASIUL, B. Efficiency of dynamic content adaptation based on semantic description of web service call context. In *MILCOM 2012 - 2012 IEEE Military Communications Conference* (Oct 2012), pp. 1–6. 214

[30] SURI, N., MORELLI, A., KOVACH, J., SADLER, L., AND WINKLER, R. Agile computing middleware support for service-oriented computing over tactical networks. In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)* (May 2015), pp. 1–5. 16, 214

[31] THE APACHE SOFTWARE FOUNDATION: HTTPS://JENA.APACHE.ORG/. 224

[32] TRIVELLATO, D., ZANNONE, N., GLAUNDRUP, M., SKOWRONEK, J., AND ETALLE, S. A semantic security framework for systems of systems. *International journal of cooperative information systems 22*, 01 (2013), 1350004. 20, 84, 143, 165, 189, 190, 215

[33] USZOK, A., BRADSHAW, J., JEFFERS, R., SURI, N., HAYES, P., BREEDY, M., BUNCH, L., JOHNSON, M., KULKARNI, S., AND LOTT, J. Kaos policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement. In *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks* (June 2003), pp. 93–96. 143, 165, 215

[34] VASILEIOS, G., WOLTHUSEN, S. D., FLIZIKOWSKI, A., STACHOWICZ, A., NOGALSKI, D., GLEBA, K., AND SLIWA, J. Interoperability of security and quality of service policies over tactical soa. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)* (Dec 2016), pp. 1–7. 63, 103, 146, 214, 227