Security Requirements for the Deployment of Services Across Tactical SOA

Vasileios Gkioulos[1] and Stephen D. Wolthusen[1,2]

[1] Norwegian Information Security Laboratory, Norwegian University of Science and Technology, Norway
{vasileios.gkioulos,stephen.wolthusen}@ntnu.no
[2] School of Mathematics and Information Security, Royal Holloway, University of London, United Kingdom

Abstract. Service Oriented Architectures (SOA) 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.

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 (Area of Operations). 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 Mobile Ad-hoc (MANET) 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 NEC (Network Enabled Capability) and

NCW (Network Centric Warfare) 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 [1–9] within the EDA (European Defence Agency) project TACTICS focused on the investigation of suitable techniques, for the deployment of such mechanisms across contemporary C2 (Command and Control) and C4I (Command, Control, Communication, Computers and Intelligence) 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 Tactical Service Infrastructure (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 methodology 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 2 introduces related work. Sections 3 and 4 present the assets, and direct or transitive threats that emerged from the analysis of the aforementioned scenarios. Finally, sections 5 and 6 highlight the identified operational and technical requirements for the development of services within tactical SOA.

2 Related Work

A multitude of earlier studies was focused on the investigation of security aspects related to commercial MANETS [10–14]. 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. [15] 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. [16] 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 [17] 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. [18] 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 aspects, the authors provide a thorough presentation of the requirements of tactical networks and the capabilities of current technologies towards their realisation.

Wang et al. [19] 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. [20] 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 [21–29] 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 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 rely 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. 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 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.

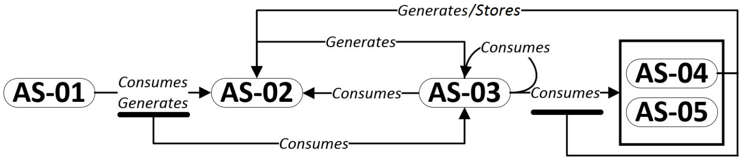

Fig. 1. Interactions across the identified assets.

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 ENISA (European Union Agency for Network and Information Security) threat taxonomy [30]. Thus, filtering threats related to SOA across tactical environments, and identifying the affected assets in conjunction with the model presented in section 3, allowed the mapping of transitive impact propagation. The identified interactions can be seen in table 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 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.

5 Identified Operational Requirements

Setting the services as the core network element instead of the radio links, impose 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 [1], 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 principals 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 information 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.

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).

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.

References

1. Gkioulos, V., Wolthusen, S.D.: Securing Tactical Service Oriented Architectures. 2nd International Conference on Security of Smart cities, Industrial Control System and Communications (SSIC) (2016)
2. Gkioulos, V., Wolthusen, S.D.: Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks. Norwegian Information Security Conference 2015 (NISK-2015)
3. Gkioulos, V., Wolthusen, S.D.: Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures. Advances in Networking Systems Architectures, Security, and Applications - of Springer's Advances in Intelligent Systems and Computing (2015)
4. Gkioulos, V., Wolthusen, S.D.: Reconciliation of Ontologically Defined Security Policies for Tactical Service Oriented Architectures. International Conference on Future Network Systems and Security-FNSS (2016)
5. Gkioulos, V., Wolthusen, S.D.: A Security Policy Infrastructure for Tactical Service Oriented Architectures. 2nd Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS 2016), in conjunction with ESORICS 2016
6. Gkioulos, V., Wolthusen, S.D., Flizikowski, A., Stachowicz, A., Nogalski, D., Gleba, K., Sliwa, J.: Interoperability of Security and Quality of Service Policies Over Tactical SOA. IEEE Symposium on Computational Intelligence for Security and Defense Applications (IEEE CISDA 2016) - IEEE Symposium Series on Computational Intelligence (IEEE SSCI 2016) (2016)
7. Aloisio, A., Autili, M., D'Angelo, A., Viidanoja, A., Leguay, J., Ginzler, T., Lampe, T., Spagnolo, L., Wolthusen, S.D., Flizikowski, A., Sliwa, J.: TACTICS: tactical service oriented architecture. CoRR **abs/1504.07578** (2015)
8. Lampe, T.A., Prasse, C., Diefenbach, A., Ginzler, T., Sliwa, J., McLaughlin, S.: TACTICS TSI Architecture. International Conference on Military Communications and Information Systems ICMCIS (2016)
9. Lopes, R.R.F., Wolthusen, S.D.: Distributed security policies for service-oriented architectures over tactical networks. In: Military Communications Conference, MILCOM 2015 - 2015 IEEE. (Oct 2015) 1548–1553
10. Priya, S.B., Theebendra, C.: A study on security challenges in mobile adhoc networks. (2016)
11. Kauser, S.H., Kumar, P.A.: Manet: Services, parameters, applications, attacks & challenges. (2016)

12. Patidar, D., 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. ICTCS '16, New York, NY, USA, ACM (2016) 81:1–81:5
13. Kannammal, A., 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) 1–7
14. Rai, B., Jain, P.A.: Survey of attacks and security schemes in manet. Universal Journal of Computers & Technology (UJCT) **1**(1) (2016)
15. Bass, T., 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. Volume 1., IEEE (2001) 64–70
16. Kidston, D., Li, L., Tang, H., Mason, P.: Mitigating security threats in tactical networks. Technical report, DTIC Document (2010)
17. Jacobs, S.: Tactical network security. In: Military Communications Conference Proceedings, 1999. MILCOM 1999. IEEE. Volume 1. (1999) 651–655 vol.1
18. Burbank, J.L., Chimento, P.F., Haberman, B.K., Kasch, W.T.: Key challenges of military tactical networking and the elusive promise of manet technology. Comm. Mag. **44**(11) (November 2006) 39–45
19. Wang, H., Wang, Y., 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) 312–315
20. Kidston, D., Li, L.: Management through cross-layer design in mobile tactical networks. In: 2010 IEEE Network Operations and Management Symposium - NOMS 2010. (April 2010) 890–893
21. Lund, K., Eggen, A., Hadzic, D., Hafsoe, T., Johnsen, F.T.: Using web services to realize service oriented architecture in military communication networks. IEEE Communications Magazine **45**(10) (October 2007) 47–53
22. Birman, K., Hillman, R., Pleisch, S.: Building net-centric military applications over service oriented architectures (2005)
23. Suri, N.: Dynamic service-oriented architectures for tactical edge networks. In: Proceedings of the 4th Workshop on Emerging Web Services Technology. WEWST '09, New York, NY, USA, ACM (2009) 3–10
24. Russell, D., Xu, J.: Service oriented architectures in the delivery of capability. Proc. of Systems Engineering for Future Capability (2007)
25. Croom Jr, C.E.: Service-oriented architectures in net-centric operations. Technical report, DTIC Document (2006)
26. Johnsen, F.T., Flathagen, J., Hafse, T.: Pervasive service discovery across heterogeneous tactical networks. In: MILCOM 2009 - 2009 IEEE Military Communications Conference. (Oct 2009) 1–8
27. Russell, D., Xu, J.: Service oriented architectures in the provision of military capability. In: UK e-Science All Hands Meeting, Citeseer (2007)
28. Russell, D., Looker, N., Liu, L., 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), IEEE (2008) 33–41
29. Candolin, C.: A security framework for service oriented architectures. In: MILCOM 2007 - IEEE Military Communications Conference. (Oct 2007) 1–6
30. Marinos, L., ENISA: ENISA Threat Taxonomy A tool for structuring threat information INITIAL VERSION 1.0. Technical report (JANUARY 2016)