future internet

MDPI

Review

A Systematic Literature Review on Military Software Defined Networks

Vasileios Gkioulos *,†,‡, Håkon Gunleifsen ‡ and Goitom Kahsay Weldehawaryat ‡

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik 2815, Norway; hakon.gunleifsen2@ntnu.no (H.G.); goitom.weldehawaryat@ntnu.no (G.K.W.)

* Correspondence: vasileios.gkioulos@ntnu.no; Tel.: +47-61135162

† Current address: NTNU i Gjøvik, Teknologiveien 22, Gjøvik 2815, Norway.

‡ These authors contributed equally to this work.

Received: 24 August 2018; Accepted: 7 September 2018; Published: 12 September 2018

Abstract: Software Defined Networking (SDN) is an evolving network architecture paradigm that focuses on the separation of control and data planes. SDN receives increasing attention both from academia and industry, across a multitude of application domains. In this article, we examine the current state of obtained knowledge on military SDN by conducting a systematic literature review (SLR). Through this work, we seek to evaluate the current state of the art in terms of research tracks, publications, methods, trends, and most active research areas. Accordingly, we utilize these findings for consolidating the areas of past and current research on the examined application domain, and propose directions for future research.

Keywords: military networks; network function virtualization; SDN; software defined networks; software defined radio; systematic literature review; survey; tactical networks; wireless sensor networks

1. Introduction

Certain types of application domains rely fully or partially on constrained dynamic networks due to technical, physical or other limitations of financial and regulatory nature. Military and emergency response networks are examples of such application domains, while their study is further motivated due to the nature of the scenarios and areas of their utilization. Four levels of command have been defined across military operations, namely (i) political, (ii) strategic, (iii) operational, and (iv) tactical. The infrastructure serving the three higher levels of command typically relies on comparatively over-provisioned wire-line and wireless networks. Contrary to that, the networks serving the tactical level mainly consist of constrained mobile devices, with self configuring characteristics, and connectivity limitation both locally and towards the infrastructure serving the other levels.

In addition to bandwidth limitations and unstable connections, military networks require tailored security solutions, which consequently create additional overhead for the network and can influence the stability of the connections. The capabilities of the nodes are also often limited by low battery life, low storage capacity and limited CPU power. These networks are characterized as Disconnected, Intermittent and Limited networks (DIL) or disruption-tolerant networks (DTN). Trends of data-centric solutions in the civil domain such as Software Defined Networks (SDN) and Network Function Virtualization (NFV) execute the network control in a centralized manner, while CPU intensive services are distributed. These principles have the potential of satisfying the network constraints of military networks. Hence, the main idea behind this literature review was to discover how these trends of SDN have been adopted to constrained military networks, and how they can contribute to solve their operational challenges.

Although not all types of tactical nodes are constrained, and sections of the network may operate under a non-constrained mode, communication across the tactical network and towards higher levels of command must be optimized for the support of the required military capabilities. Accordingly, this generates strict requirements to the deployed service delivery and policy based management systems, both in terms of security and quality of service. This is aggravated by environmental limitations, which arise due to the aforementioned constrained and dynamic nature of military operations. Accordingly, such deployed supporting mechanisms are affected, since they have to operate within severe constraints, in terms of the locally achievable bit-rate and throughput, high packet loss and packet loss variability, asymmetric link characteristics, and high rate of change and unpredictability within the network topology graph. Furthermore, currently used network devices commonly integrate functions related both to the control and data planes. The network control planes are often distributed to enable the networks to operate autonomously. However, SDN opens up for moving the enforcement of policy management and QoS (Quality of Service) control from a service application oriented control plane to a network oriented control plane.

Software Defined Networking is defined as the concept of separating the control plane and the data plane. Practically, this separation results in a clear distinction between a network controller and the distributed network devices. However, the separation of the planes is implemented in various versions of SDN where the level of centralized control slightly differs. These different SDN protocols also have different application domains and can contribute to multiple layers in the networking stack. SDN can for example both be a tool to enable distributed DDoS protection and it can be a control plane for routing network traffic. The main part of this literature review classifies SDN into different categories with respect to how SDN can be an enabler for network traffic routing.

The second part of this literature review discusses SDN related technologies such as Network Function Virtualization and Software Defined Radio that we refer to as additional contributions, as the principles of separating data and control planes have also been adopted by Software Defined Radios. Compared to traditional SDN such as OpenFlow, SDR differs because it works on layer 1 and 2 and focuses more on virtualized software. Correspondingly, other SDN related technologies use similar principles by virtualizing both networks and software, raising the question on which technologies are defined as SDN and what SDN really is. This literature review does not aim to review SDN or define SDN, but aims to review the types of SDN technologies that have been adopted to military networks. Hence, the second part of this review classifies SDN related technologies in a military context.

Historically the first SDN research from Stanford in 2008 aimed to provide a centralized controller capable of making global forwarding decisions based on packet header attributes. The main idea was to reduce the need of expensive network devices and advanced routing protocols, with a centralized controller making all forwarding decisions. However, in modern networks, a hybrid SDN approach is used to face the challenges of legacy management and legacy control. Hence, modern routers can have multiple instances of SDN domains where we face new challenges of inter domain communication between network controllers. Not only control commands to network devises are important, but orchestration of controllers and control messages between the controllers. The multiple levels of command in military networks indicate a network topology associated with multiple SDN domains, while the results of this SLR also indicate that securing such topologies is a significant future research challenge.

This study is a systematic literature review on military SDN and not a comparative survey of SDN technologies at large, as comprehensive studies with this focus already exist (see Section 2). Therefore, the scope of our study covers only research articles that include SDN in a military context, seeking to establish and examine the current state of obtained knowledge on military SDN. This implies that papers which include SDN technologies but not within a military context are omitted by this review. Section 3 includes a detailed description of the method followed for conducting this SLR. This work seeks to evaluate the current state of the art in terms of research tracks, publications, methods, trends, and most active research areas, with focus on military SDN. The remainder of this article is structured as follows: Section 2 presents related work, while Section 3 presents the utilized research method for this systematic literature review. Section 4 contains a comprehensive discussion over identified significant research contributions, while Section 5 discuss additional contributions. Finally, Section 6 provides a statistical analysis of our findings and the corresponding metrics, while Section 7 analyses directions of future work, and Section 8 includes our conclusions.

2. Related Work

To the best of the authors' knowledge, no systematic literature review has been conducted earlier on the topic of military SDN. Nevertheless, it must be noted that some of the articles that we encountered, and present in our study, include comprehensive related work sections. In lack of such an earlier study, we have identified a set of stimulating previous surveys and literature reviews, focusing on aspects related to SDN with generic scope, or application domains distinct to the one discussed here. These articles have been utilized as a basis for our study in terms related to research methods, sources, and presentation of results.

Horvath et al. [1] conducted a systematic literature review on challenges and effects of SDN until June 2014, identifying 44 relevant articles. The authors highlight and discuss topics such as decoupling hardware from software, network management, programmability, and maintenance. Accordingly, they classify the articles in terms related to their contents, as addressing or discussing SDN challenges (6: know-how, 10: demand, 19: implementation), and effects (27: features, 15: management, 10: economic factors). After an extended analysis on these topics, the authors draw related conclusions including that: *"the analyzed papers mostly describe software defined networking on a very detailed mathematical and technological basis, making it very hard for enterprises and organizations to assess if the technology can have a specific business impact."*.

Govindarajan et al. [2] provided a literature review on SDN research topics, challenges and solutions, providing a classification of research challenges in SDN, corresponding ongoing research efforts, and a comparison of those. Although this study is not formated as a systematic literature review, it provides a comprehensive overview and discussion of the utilized technologies, methods and open issues, such as load balancing, scalability, and security. Furthermore, Xia et al. [3] provided a survey on SDN at 2015, discussing the latest developments in this research area at that time. The article is not examining in depth specific topics, but it provides a generic and comprehensive overview of SDN theory, but also related research efforts on a wide variety of topics, such as processing optimization, policy and rule validation, network virtualization, and maintenance.

Alsmadi et al. [4] conducted a systematic literature review on SDN, seeking to classify research papers published on SDN, investigate existing challenges and oportunities, highlight the evolution of the SDN paradigm, and identify the main contributors in the area. This article has been identified to present the most concrete methodology and presentation of results among the related literature reviews, therefore elements of our methodology (see Section 3) across the undertaken studies for this article have been influenced by its structure. Another well structured and highly influential (605 citations by December 2017) survey on SDN, has been conducted by Kreutz et al. [5]. As described by the authors *"This paper offers a comprehensive survey of software-defined networking covering its context, rationale, main concepts, distinctive features, and future challenges."* The authors begin with a comprehensive description of the SDN paradigm discussing elements such as terminology, definitions, the standardization process, and historical overview. Furthermore, they provide a bottom up survey of existing studies across architectural elements such as: programming languages, network applications, interfaces, operating systems, and infrastructure. Finally, this article provides a summary of ongoing research efforts and challenges in eight categories, including resilience and scalability, security and dependability, controller platforms.

Jammal et al. [6], provided a survey on SDN, focusing on the analysis of the current state of the art and research challenges. The authors focused on elements such as the open-flow architecture, network function virtualization, SDN applications, challenges and existing solutions. Other influential surveys on the field of SDN include Lopes et al. [7] for trends and challenges on programming for SDN environments, Goel et al. [8] for network virtualization techniques, Jarraya et al. [9] on SDN taxonomies, research directions, challenges, and recomendations for future work, and Mendonca et al. [10] for programmable networks with an emphasis on SDN. Furthermore, Bennesby et al. [11] provided a study on current approaches for reducing BGP (Border Gateway Protocol) appropriate inter-domain routing convergence delay on the Internet, Hu et al. [12] focused specifically on SDN/OpenFlow designs and architectures, while Anderson et al. [13] analysed resilience supporting mechanisms for SDN.

3. Research Method

For the execution of this study we utilized the method described by Okoli and Schabram [14], for conducting systematic literature reviews of information systems research, adopting additional useful components from the studies presented in Section 2, and particularly articles [4,5]. This method is comprised of the following distinct steps:

1. "*Purpose of the literature review:*"

   For our study, the "Purpose of the literature review" has been defined as: to analyze the current state of the art within the topic of military SDN, in terms of research tracks, publications, methods, trends, and to make recommendations for future research. Accordingly the executed tasks seek to satisfy the following explicit goals:

   (a) To identify and classify the research papers published on the topic of military SDN;
   (b) To analyze and evaluate the research papers published on the topic of military SDN and summarize the related research results;
   (c) To identify the most active and influential researchers, groups, conferences, and journals, on military SDN;
   (d) To identify the current main focus areas within the topic of military SDN;
   (e) To make recommendations for future research.

2. "*Searching for the literature:*"

   The identification and extraction of related literature was finalized on 15 August 2018, in the following academic research databases: IEEE Xplore, ACM Digital Library, ResearchGate, Microsoft Academic Search, ScienceDirect, CiteSeerX, Scopus, ProQuest, BIBSYS, and Semantic Scholar. Furthermore, this process has been executed by explicit combination of two groups of key-words, where the first group of terms was related to the technology (i.e., SDN, Software Defined Networks) and the second on the application domain (i.e., Military, Strategic, Tactical), providing a total of six combinations for each database.

   Seeking to maximize comprehensiveness and extract the whole of related articles, we transferred the weight of inclusion on the next step (practical screening), by selecting to utilize the majority of academic research databases (accepting the risk of multiple duplicate outputs), and selecting wide terms as key-words (accepting the risk of outputs with limited relevance to the purpose of this literature review).

3. "*Practical screening:*"

   For the selection of articles and mitigation of the aforementioned risks, we defined several exclusion criteria and rounds, as follows:

   (a) Articles published in languages other than English have been excluded.
   (b) Duplicate articles occurring across the examined scientific databases have been excluded.
   (c) Reports, presentations, editorials, and posters have been excluded, while we selected only scientific articles published in conferences, workshops, and journals. Furthermore, we have included PhD, and MSc thesis of significant relevance to the examined topic.

(d) The article must be directly related to SDN or in combination with relevant fields, such as NFV (Network Function Virtualization) or SDR (Software Defined Radio), but not only on related fields without mentioning SDN.

(e) No exclusion criteria have been defined in accordance with the year of publication, publisher, and author affiliation.

4. *"Quality appraisal:"*

   The initial database screening, with the search method and exclusion criteria described in the two previous paragraphs, resulted in 927 entries. At this stage, the authors defined and individually applied an application domain related filter, seeking to identify scientific contributions with relevance to the purpose of this literature review. This filter was defined as:

   "The article must be directed to military networks or clearly mention military networks as a potential application domain for the presented contribution."

   Consolidating the three individual recommendations resulted in the final list of entries that are presented in this literature review. Consequently, these articles have been independently evaluated in terms of relevance, significance, and impact. Consolidating the three individual recommendations resulted in the significant research contributions (presented in Section 4) and additional contributions (presented in Section 5). Finally, the last evaluation round was related to the categorization of the identified contributions, for facilitating the synthesis of our study and the presentation of results.

5. *"Data extraction:"*

   The data extraction and analysis of the identified articles have been conducted in accordance with a review form for maintaining completeness and consistency. This form has been established in accordance with official review forms utilized for internationally established scientific conferences, enhanced with suitable components for the extraction of substantial research results and contributions.

6. *"Synthesis of studies:"*

   For the synthesis of our study and iterative development of literature mapping, we utilized the qualitative material gathered through steps 5 and 6. Accordingly, the two groups of articles have been further categorized according to their focus areas and analyzed as presented in Sections 4 and 5. Furthermore, we collected quantitative data for the examined articles, allowing the extraction of statistical metrics as presented in Section 6. Finally, combining the results of these sections allowed us to provide an overall analysis of the examined ecosystem, and extract recommendations for future work, as presented in Section 7.

7. *"Writing the review:"*

   Writing this systematic literature review has been conducted in accordance with the standard principles for writing research articles, utilizing the method described by Okoli and Schabram [14] and by adopting additional useful components from the studies presented in Section 2. Furthermore, this section provides functional details that allow reproducing our results, or updating this study at a later time.

The number of identified entries across the stages of conducting this literature review is as follows:

- Entries identified through database searching: 967,
- Entries identified through citation back-tracing: 94,
- Records after removal of duplicates: 927,
- Records after initial screening: 134,
- Full-text articles assessed: 134,
- Studies assessed as significant contributions: 43,
- Studies assessed as additional contributions: 91.

4. Identified Significant Research Contributions

The extracted articles which have been identified to provide significant research contributions on the examined topic are presented in Table 1. Furthermore, in this section, we discuss these articles, categorizing them in accordance with their research contributions. The articles have been classified in accordance with their application domain (as mentioned by the articles' authors: aerial, coalition, distributed, heterogeneous, military, mission critical, mobile ad hoc, naval, and tactical networks), their research contribution (as extracted: architectures, basic evaluation, tools, services, control systems), their scope (as extracted: basic evaluation, design and management, monitoring and control, policy based management, resource sharing, security, and simulations), the layer that the contribution is focused on (as extracted: all, application, control, physical), and finally with respect to the extent of their focus on security (as extracted: no, yes, only mentioned).

4.1. Architectures

A multitude of articles in this category investigate topics related to network monitoring and control. Nobre et al. [15] proposed a battlefield networking architecture, enabling the deployment of SDN based applications and policies. The article examines in detail the benefits and disadvantages of (i) centralized, (ii) hierarchical, and (iii) federated approaches, comparing the two later and discussing in detail the supported policy based management solutions. Furthermore, the authors briefly discuss security implications and proceed by examining two use cases related to (i) bidirectional video streaming, and (ii) task coordination. Overall, the article is comprehensive and consistent with current research trends, although further evaluation is suggested. Furthermore, Zacarias et al. [16] proposed a joint exploration of the SDN and Delay Tolerant Network (DNT) concepts, in order to address the specific constraints and problems arising at the last-mile Tactical Edge Networking (TEN). The proposed approach takes under consideration the resource constrained devices used by troops in the field, while it benefits from the programmability of SDN, and the ability of DTN to handle link outages. Two use cases are examined in order to highlight the applicability of the proposed architecture. The first sets out a scenario that highlights some of the SDN features within network partitions supporting a non-elastic application. The second use case deals with the management of communication between heterogeneous nodes in the TEN, which spread across different partitions.

Mihailescu et al. [17] suggested a prototype framework for (i) network control, (ii) traffic prioritization management, and (iii) radio/protocol integration, with the use of SDN for emergency response and military networks. Initially, the article contributes with a two-tier hierarchical SDN controller setup, which exposes a modular interface for the management of wireless networks. Furthermore, the authors proposed a framework that allows the integration and interoperability across distinct wireless network technologies. Both frameworks are presented in detail, related to the desired functionalities of (i) traffic prioritization, (ii) remote network management, and (iii) multiple radio integration. Accordingly, the authors present the results of their initial evaluation process, presenting a small scale prototype implementation. The article investigates an interesting research path, but further evaluation and development is required, since the presented validation approach is small in scale for comprehensively highlighting the overall benefits.

Moreover, Phemius et al. [18] described an architectural framework for traffic management in tactical networks, combining elements of Mobile Edge Cloud (MED) and SDN, to allow optimal network reactivity to the wireless link variations. The proposed framework can be decomposed into four layers, namely: the (i) "waveform layer" which consists of the multiple deployed programmable radios, the (ii) "SDN layer" which contains a virtual switch and the SDN controller, the (iii) "application management layer" which is mapped to the MED where the applications run, and the (iv) "mobile edge controller" which is a module that bridges the other three layers. Channel state information are periodically measured and aggregated at the controller, which routes the traffic in accordance with these information and dedicated policies deployed within the "mobile edge controller", in order to detect network saturation or bottlenecks and react accordingly. The authors have implemented the proposed architecture in a test-bed that emulates a platoon level tactical network, abstracting the backbone infrastructure, towards the validation of their results. The utilized test-bed is described in detail within the article, while two distinct scenarios are used for validation purposes that primarily relate to network management. Further validation is proposed, given the limited size of the examined topology, but also limitations related to node mobility and communication patterns, which have not been captured extensively under the realistic characteristics of tactical deployments. Nonetheless, the experimentation method is sound and provides viable insights towards future work, which as the authors suggest will include extended configurations.

White et al. [19] proposed an SND and Network Function Virtualization (NFV) based architecture, within the highly mobile environment of Unamaned Aerial Vehicles (UAV) infrastructures. The proposed architecture aims at (i) improving situational awareness for pilots and payload operators during UAV missions, (ii) increasing continuity of services in deployments with weak backbone infrastructure, (iii) reduction of latency in applications related to situational awareness, and (iv) reduction of the requirements imposed on the backbone infrastructure in cases of outages or traffic spikes. Each UAV is defined as a host, with mobile ground vehicles operating as switches, which route traffic towards the pilots in command and mission payload operators, in accordance with predefined OpenFlow rules. The chained containers hosting the VNFs (Virtual Network Functions) are located in the ground vehicles, while the SDN controller is located at the central command center. The authors implement their architecture with Linux based chained containers for instantiation of the VNFs and the Python SDN controller. Validating their architecture, the authors utilize scenarios that focus on pilot saturation with alerts. The results support an improvement of situational awareness, due to the programmability of reports related to emerging challenges, and an overall improvement in terms of resilience. Furthermore, high mobility patterns are supported through the integrated distributed selection of resilient links with sufficient capacity and availability.

Kumar et al. [20] describe a framework that leverages the benefits of the SDN paradigm, in order to guarantee end-to-end timing constraints in safety critical Real Time Systems (RTS). The advantage of using SDN in such systems is that it provides a centralized mechanism for developing and managing the system. Furthermore, such a global view is useful in providing the end-to-end delay limitation guarantees that are required. As the authors suggest, another advantage is that the hardware/software resources needed to implement the proposed framework are limited. A prototype is implemented as an application that uses the northbound Application Programming Interface (API) for the controller, which accepts a specification of flows that contain a classification, bandwidth requirements, and the delay constraints of each individual flow. The proposed solution is evaluated using the following two methods: (i) a performance exploration of the path layout algorithm design, and (ii) an empirical evaluation using Mininet, which demonstrate the effectiveness of the end-to-end delay guaranteeing mechanisms. As noted, most hardware switches limit the maximum number of queues that can be allocated to flows, while the presented realization mechanism reserves only one queue per port for each flow, leading to the depletion of available queues. Moreover, Spencer and Willink [21] provide a basic evaluation of SDN within coalition networks, and address research challenges related to the dynamic ecosystem of military networks. In particular, the authors focus on dynamic wireless networks and network controller topologies, by presenting the identified challenges and vulnerabilities. The challenges are reflected by the constraints of military networks such as (i) limited bandwidth, (ii) unreliable wireless connectivity, (iii) dependencies of the network controllers, (iv) east–west control plane channels, and (v) data integrity in open networks. Overall, the main contribution of this article, is to present a summary of related challenges identified within the proceedings of a TTCP-C3I (The Technical Cooperation Program—Command, Control, Communications and Information Systems) group.

Table 1. Identified significant research contributions.

Article	Application Domain	Contribution	Scope	Layer	Security
[22]	Heterogeneous networks	Architectures	Design and management	Control	No
[19]	Aerial networks	Architectures	Monitoring and control	Control	Mentioned
[23]	Aerial networks	Control systems	Monitoring and control	Control	No
[24]	Military networks	Control systems	Policy based management	Control	Yes
[25]	Tactical networks	Services	Design and management	Control	Yes
[26]	Military networks	Control systems	Design and management	Application	Mentioned
[27]	Military networks	Services	Design and management	Application	Mentioned
[18]	Tactical networks	Architectures	Monitoring and control	Control	Mentioned
[16]	Tactical networks	Architectures	Monitoring and control	Control	Mentioned
[28]	Coalition networks	Control systems	Resource sharing	All	Mentioned
[29]	Military networks	Control systems	Policy based management	Application	Yes
[30]	Military networks	Control systems	Policy based management and Resource sharing	Application	Yes
[20]	Tactical networks	Architectures	Monitoring and control	Control	Mentioned
[31]	Coalition networks	Control systems	Resource sharing	Control	Yes
[32]	Mobile ad hoc networks	Control systems	Monitoring and control	Control	Yes
[33]	Mission critical networks	Control systems	Monitoring and control	Control	Mentioned
[34]	Distributed networks	Tools	Security	Application	Yes
[17]	Military networks	Architectures	Monitoring and control	Control	No
[35]	Naval networks	Basic evaluation	Basic evaluation	Control	Mentioned
[36]	Tactical networks	Basic evaluation	Basic evaluation	Control	No
[37]	Tactical networks	Basic evaluation	Basic evaluation	Control	Yes
[38]	Military networks	Tools	Simulations	Control	Mentioned
[39]	Military networks	Control systems	Policy based management and Resource sharing	Control	Yes
[40]	Coalition networks	Control systems	Security	Control	Yes
[41]	Tactical networks	Control systems	Design and management	Control	No
[42]	Coalition networks	Control systems	Monitoring and control	Control	Yes
[43]	Naval networks	Control systems	Monitoring and control	Control	No
[21]	Coalition networks	Architectures	Basic evaluation	Control	Yes
[44]	Military networks	Tools	Security	Physical	Yes

Table 1. *Cont.*

Article	Application Domain	Contribution	Scope	Layer	Security
[45]	Naval networks	Control systems	Monitoring and control	Physical	Mentioned
[15]	Tactical networks	Architectures	Monitoring and control	Control	Yes
[46]	Tactical networks	Tools	Basic evaluation	Control	Yes
[47]	Military networks	Control systems	Policy based management	Control	Yes
[48]	Military networks	Tools	Security	Physical	Yes
[49]	Tactical networks	Tools	Monitoring and control	Control	No
[50]	Tactical networks	Control systems	Monitoring and control	Control	Mentioned
[51]	Tactical networks	Control systems	Monitoring and control	Control	No
[52]	Tactical networks	Control systems	Basic evaluation	Control	No
[53]	Tactical networks	Tools	Simulations	Application	Yes
[54]	Military networks	Services	Design and management	Application	No
[55]	Mobile ad hoc networks	Control systems	Monitoring and control	Control	Yes
[56]	Naval networks	Control systems	Monitoring and control	Control	No
[57]	Coalition networks	Control systems	Basic evaluation	Control	Yes

Finally, investigating design and management systems, Elgendi et al. [22] propose a three-tiered SDN architecture of heterogeneous and highly dense low-power femtocells at the tactical edge, aiming to satisfy the increasing capacity demands while simplifying the management overhead and increasing scalability. The proposed architecture consists of (i) the physical layer, based on dense low-power femtocells, (ii) the control layer which acts as a local controller, and (iii) a management layer which acts as a global controller. Routing and Quality of Service (QoS) decisions are made at the control layer in coordination with the management layer, the latter also being responsible for handovers. Furthermore, the authors focus on mobility and session management, describing in detail the developed sequential processes and required subsystems. The authors use the Mininet simulator in order to validate their results and evaluate the suggested architecture. The results suggest that within the utilized scenario, the proposed three-tier architecture reduces the delay, while increasing the throughput. Furthermore, the performance of the suggested architecture is evaluated in different mobility scenarios, suggesting that in low speeds a smooth flow rate among femtocells is achievable, while in speeds over 30 km/h the use of hotspots or macrocells is required in order to enhance connectivity. The utilized simulation scenarios are aligned with the high level architectural requirements of tactical networks, although limitations in terms of the deployed number of nodes and mobility models are visible.

4.2. Control Systems

As in the previous subsection, the majority of articles with research contribution related to control systems have a scope that is targeted towards monitoring and control. Nazari et al. [45] proposed an SDN framework for a fleet of ships that relies on multiple satellite communication systems for on-board communications. The SDN framework addresses practical issues in current naval networks, such as sharing and load balancing of multiple communication links, as well as overcoming constraints related to bandwidth limitations. To overcome link intermittence and outage, the authors propose the use of Multi Path Transmission Control Protocol (MPTCP), which improves end-to-end data delivery by creating several sub-flows under a TCP session. The cooperation between MPTCP and the SDN controller leads to an agile, bandwidth efficient, and robust naval network. The authors conducted SDN-SAT performance evaluation tests, using the Mininet emulator on a commodity laptop, where the SDN-SAT controller protocol and the MPTCP Linux kernel run on the same machine. Open vSwitch is used in order to emulate the switches, while the initial results are promising in terms of functionality support and performance, although the performance of SDN and MPTCP is not addressed when the underlying network consists of a large number of ship nodes. Additionally, Du et al. [56] designed and implemented SDN-SAT traffic optimization algorithms and associated SDN protocols on the SDN network emulator Mininet, with focus on naval surface fleets utilizing satelite communication systems. The SDN emulation testbed uses Mininet 2.1.0, Floodlight 1.2 (for the controller), OpenFlow 1.3 Software (for the switch) and MPTCP Linux Kernel Implementation v0.90. The Flow Deviation Method (FDM) is used as a network-wide optimal load-balancing solution that maximizes total throughput and minimizes traffic flow delay and jitter, while this optimization is carried out via a central controller in a Software Defined Networking (SDN) framework. It must be noted that the FDM algorithm convergence time and control overhead (in terms of SATCOM bandwidth) exchanged between SDN switches and their controller are not addressed in this work.

Also focusing on naval networks, Lee et al. [43] proposed an SDN based Naval Ship System (NSS) and an algorithm called "Real-time Transmission via Flow-rate-control" (RTF) for environment specific optimization. With the proposed algorithm, SDN is employed as a new network architecture for the NSS, in order to control the QoS of real-time data over a tactical scenario. An optimization problem in terms of delay and prioritization is formulated, in order to achieve real-time transmission over SDN based NSSs. Consequently, a dual-decomposition method is applied in order to solve the non-convex optimization, while the authors measure the performance of the proposed solution by employing a tailored Floodlight SDN controller. The proposed SDN-based NSS is virtually established using

Mininet, in order to verify the efficiency of the algorithm. The network topology used for the executed experiments is composed of 500 nodes and eight gateways, while Floodlight V1.1 and OpenVswitch are utilized for the implementation. Finally, the traffic of each node is generated individually, by utilizing the Hierarchical Multi-level On/Off Source (HMLOS) traffic model.

In respect to coalition operations, McLaughlin et al. [42] proposed an SDN based framework for the mobility management of operational nodes within coalition military environments. The examined problem is analyzed in depth by the authors, providing significant insights in terms of operational, functional, and security constraints and requirements. The proposed framework seeks to implement Protected Core Networking (PCN) utilizing SDN, where PCN separates the transport and information domains, towards multinational networks that provide flexible and secure transport services. The authors describe in detail three logical topologies for the SDN controller, namely: (i) centralized, (ii) partially-meshed, and (iii) extension to static hosts.

Within the same application domain, Pham et al. [31] summarized a set of research challenges related to Content Based Networking (CBN) in military coalition networks. As presented by the authors, in a joint military operation, the key focus is to bring together different partners into a single mission, maintaining the ability to securely share data across the distinct teams. Furthermore, it is required that the network operators are capable of performing analytics and maintain service related situational awareness in a resource constrained network. SDN is promoted by the authors as an enabler for CBN in respect of easing the complexity, and allowing the dynamic discovery of distributed information. However, centralized network control, such as OpenFlow, does not fit with disruptive networks. The paper suggests placing future research focus on: (i) hybrid SDN in order to allow network independence from the controllers, (ii) east–west control plane communication between network controllers, (iii) security implications related to dynamic distributed services, (iv) content aware networking by mapping the service request to the network control, and (v) distributed analysis in order to derive human situational understanding.

Also focusing on coalition networks, Mishra et al. [40] examined how the principles of SDN can be utilized in order to improve cyber situational awareness in coalition environments within military networks. The authors discuss the adaptation of the Observe, Orient, Decide, Act (OODA) loop within SDN in order to improve security awareness. The OODA loop describes a decision-making process and is reflected in an SDN controller application. The authors also suggest that an east–west communication protocol is required for controllers to share what they have learned. The article explains comprehensively the concepts related to the OODA loop but does not provide an extensive discussion over the corresponding requirements and constraint for its adaptation on SDN. Consequently, Mishra et al. [28] examined the application of SDN across military coalition operations, proposing a mechanism for enabling dynamic Communities of Interest (CoI) within these environments, and evaluating such interoperability architectures in accordance with key performance metrics. Furthermore, this article provides a comprehensive overview of tactical communities of interest and the underlying constraints towards their deployment and management. The authors proceed by merging the two, and discussing the topic of Software Defined Coalitions (SDC), as the mechanism that is capable of facilitating the operation of dynamic tactical CoIs. Accordingly, they identify three interoperability levels, namely: (i) network, (ii) network and storage, and (iii) network, storage, and compute. They clarify that (ii) combines mechanisms from SDN and Software Defined Storage, while (iii) builds upon the concept of Software Defined Environments. Consequently, the article proposed three types of architectures, namely: (i) simplification, (ii) brokered, and (iii) federated, comparing the three in terms of complexity, trust, and standardization. The presentation and discussion of the proposed mechanisms is sound and comprehensive, although further scenario based validation/verification can be desirable.

With focus on aerial networks, Iqbal et al. [58] proposed an SDN and SDR architecture that can predict network outage in aerial networks. Under the assumption that aerial flights have fixed orbits, the authors suggest that the radio can inform the centralized controller about its future position, allowing for the flow routes and radio links to be switched in advance and prior to network outege. Hence, the availability is expected to be increased by the use of predictive SDN. The presented architecture is based on the assumption that the radio link outage can be predicted. Accordingly a corresponding architecture is proposed and tested in a virtual environment with OpenDaylight, Quagga, and OVS. The availability is tested by comparing network convergence for Open Shortest Path First (OSPF), reactive SDN (LLDP) and proactive SDN, where the proactive SDN showed maximum availability. Nevertheless, it must be noted that the proposed solution is not compared with overlay networks such as Multiprotocol Label Switching (MPLS) with segment routing.

Within the application domain of military networks, the majority of articles is focused towards policy based management. Skappel [47] presented a master thesis with the objective of testing how an SDN controller can be used as a tool for controlling traffic in a dynamic environment. This thesis shows that SDN can allow network monitoring, and utilize this input in combination with predefined policies in order to prioritize, police, ensure QoS, and dynamically adjust the flows for different controllers. Wrona et al. presented two consecutive articles withing the same application domain and scope [30,39]. Within these articles, the authors discuss content-based security policies at different levels in the OSI stack, and present a proof of concept implementation in an SDN environment. They base their security concept on content based protection and release policies developed by NATO. The principle is that an information object is not labeled by a sensitivity tag, but it is labeled by a content tag that describes the object. Access control is based on the authentication of both the user and the terminal, while if both policies are accepted then the system release the object to the user. In the SDN context, a network packet header information can also have a content label that defines a security label. Their first article shows a proof of concept implementation of the proposed solution by retrieving information from different network layers, while the second article shows how an SDN controller that calculates the whole path in the network can also make the path itself a security label. The proof of concept implementation showed that the packet forwarding path can be protected in this manner. Hence, different paths can have different security protection levels, and the forwarding path can be decided based on content and access levels.

Nguyen et al. [24] presented a short review of military policy based management methods and suggest a model for verifying, prioritizing and deploying a group of policies based on SDN. The core of the article is a graph model that detects conflicting network polices within the sum of applied network policies. The output of the model is a set of resources that a node can access. In order to detect conflicting policies, the authors suggested a step by step procedure to conform the policy and deploy it in SDN. The authors used a standard SDN controller with virtual switches to deploy policies across SDN. The core of this article relates to network policies and deconflictation, while the validation focuses primarily on policy deployment as OpenFlow rules. Moreover, Armando et al. [29] proposed a method for facilitating the specification of access control policies in accordance with the NATO—Content Based Protection and Release model (CBPR). The CBPR model is built upon the Attribute Based Access Control (ABAC) model, and supports the specification of access control policies in complex organizations and coalitions, with extended variety of deployed resources. Accordingly, the authors propose the replacement of monitor based policy enforcement with cryptographic enforcement, in order to reduce the administrative burden, and enhance performance specifically within cloud and SDNs. The suggested solution relies on Cipher text-Policy Attribute-Based Encryption (CP-ABE), for which as the authors describe "The key idea is that a user should be able to decrypt a ciphertext only if he/she holds a key associated to certain attributes, under the assumption that user keys are issued by some trusted party". Furthermore, the authors propose the adoption of this method to SDNs, for the enforcement of protection policies (during message forwarding decisions) in accordance with specific node and link attributes. The aforementioned statement is promoted as a suggestion by the authors, while deployment and validation is required.

Mulec et al. [32] proposed a distributed flow controller for mobile ad hoc networks, seeking to provide dynamic reconfiguration and to improve security. The functions of the controller are

(i) provisioning of AAA (authentication, authorization and accounting) services, (ii) flow management across the network nodes, (iii) centralized network traffic control, and (iv) enforcement of security policy. Unicast, multicast and broadcast communication is supported, while suitable mechanisms are provided for the management of topology changes. A core component of the proposed system is the selection mechanism, which establish the number of required controllers and their prioritization. This mechanism is mathematically analyzed, and tested within a test-bed consisting of seven wireless nodes providing positive initial results. The article provides a small scale validation, while further testing is recommended, primarily related to the size of the network and the tested mobility patterns. Furthermore, Poularakis et al. [55] proposed a set of novel architecture designs for SDN-enabled mobile ad hoc networks in the tactical edge, discussed the challenges raised by the ad hoc and coalition network environment, and presented corresponding solutions. The proposed approaches build on experimental evaluations, utilizing theoretical results from SDN deployments in large backbone networks. The study provides useful insights on the examined environment, yet security related aspects could benefit from further evaluation.

Qing et al. [26] described an optimization algorithm that can be used for prioritizing service requests in military operations. According to the article, when a network does not have enough resources to serve all requests, these can be prioritized based on a predefined policy. To enable service prioritization, a set of resources that are required by the service must be prioritized. In the context of SDN, this primarily concerns prioritization of traffic on network devices. The authors suggest precombining these resources into groups, and proposed an algorithm to optimize this precombination. The authors suggested two models of optimization, where the provided results show that precombination of resource dispatching improves the network performance.

Furthermore, Bouet et al. [33] proposed a DIstributed SDN Control (DISCO) plane which allows handling the distributed and heterogeneous nature of modern mission-critical networks. The proposed approach relies on a per domain organization, where each DISCO controller is in charge of an SDN domain, using a lightweight and manageable publish–subscribe mechanism for sharing aggregated local and network-wide information with neighbor SDN controllers. Furthermore, the authors demonstrate how DISCO dynamically adapts to heterogeneous network topologies, while providing classic functionalities such as end-point migration and being resilient enough to survive disruptions and attacks. The authors implement DISCO on top of Floodlight, an OpenFlow controller, and the Advanced Message Queuing Protocol (AMQP). The network is emulated using Mininet to create topologies and instantiate Open vSwitch switches and virtual hosts. Mininet is hosted on a dedicated VM (Virtual Machine) and the controllers are hosted on separate VMs. To measure performance, the authors show an evaluation of its functionalities on an emulated SDN according to two use cases: (i) inter-domain connectivity disruption and (ii) migration of a virtual machine. The results show how DISCO dynamically adapts to heterogeneous network topologies, while being resilient enough to survive disruptions and attacks, and further being able to provide classic functionalities such as end-point migration.

Additionally, Chen et al. [51] proposed a transmission framework for Software Defined-Airborn Tactical Networks with the aim of providing a fundamental infrastructure for improving the communications capability between the control and data planes. Furthermore, the authors proposed a dedicated communication protocol, aiming at transmitting the non-elastic C/D information in both a reliable and timely manner. The authors conducted a simulation for the purpose of illustrating the performance of their scheme. They built a simplified avionics network in EXata 5.1 for every aircraft, and regarded an avionics network as a node of the SD-ATN. The simplified avionics network, which is considered as the common node, includes two devices that implement the functions of the platform controller and SD-ATN transmission system, respectively. The avionics network that represents the active control node includes one more device that implements the functions of the SD-ATN controller, while the devices within an aircraft are connected through wired links. Finally, Fagervoll [50] explored how SDN can be incorporated, both physically and logically, within heterogeneous tactical networks.

Being a Master's thesis, this work provides a comprehensive introduction into the related concepts and underlying requirements, while the main contribution is focused towards the collection of network information for the establishment of topology mapping. The author evaluated three conceptual models and proposed an approach for topology mapping through local legacy routers.

4.3. Services

Three articles have a research contribution related to services, and all have a scope related to design and management. In [25], the author proposes an SDN based Network for auto-configuring network services across federated mission networks. Currently, NATO is using standard routing protocols to exchange information about both routes and services. The author suggests interconnecting OpenFlow controllers instead of using routing protocols, while the design and experimental evaluation showed a faster auto deployment of network services using SDN compared with BGP. The article is comprehensive, although not all the requirements of the design become clear. As an example, it is not known how the network controllers exchange information, and what information they have to be preconfigured with. Furthermore, Kroculick [27] discussed opportunities for applying assurance-driven design to validate the correctness of behavioral requirements for network capability insertion in the Army's network, which is becoming increasingly virtualized with extended variation in the type and number of network resources. The author utilized the CertWare tool in order to automate assurance cases, and provided an example using the claim-argument-evidence (CAE) method in the CertWare tool in order to validate the claim. Finally, Zacarias et al. [54] proposed an SDN approach for improving the quality of video streaming for military surveillance, in which multiple Unmanned Aerial Vehicles (UAVs) are employed as data providers through an SDN-enabled network. Experiments were performed considering the application of SDN in UAV-based military surveillance scenarios using Mininet-WiFi, Ryu-SDN Framework and the FFmpeg player. A SDN was used for connecting the ground vehicles, using the SDN architecture to enhance video streaming in dynamic networks with a link capacity of 100 Mbps.

4.4. Tools

With a research contribution related to tools, one article provided a basic evaluation related to tactical networks. In this, Spencer et al. [46] assessed the integration of the SDN paradigm across tactical networks, discussing the expected benefits and potential threats. The article provides a comprehensive analysis of the characteristics of tactical networks, in conjunction with an overview of the architectural and operational attributes of SDN, aligning the two by extracting the expected benefits to the tactical user. These relate primarily to enhancements of information dissemination, service delivery, and link utilization. Furthermore, the authors provide an iterative assessment methodology regarding the performance gains by such an integration, the design options in respect to tactical SDN controllers, and challenges that need to be addressed. It must be noted that no extensive validation is provided within the article referring to the proposed methodology. Therefore, it is not clear if the results of the study are exhaustive, mutually exclusive, or if there are any identified interdependencies.

Furthermore, three articles within this sub-category have a scope related to security, either directly related to military or distributed networks. Wrona et al. [44] described an OpenFlow-based test-bed for the validation of SDN security mechanisms—including both the mechanisms for protecting the SDN and the cross-layer enforcement of higher level policies, such as data-centric security policies. Such cross-layer security mechanisms are important in the context of software-defined infrastructure and implementation of new security paradigms, such as data-centric security. Furthermore, the authors demonstrate the functional correctness of the test-bed, as well as its suitability to provide validation and additional insight into the behavior of analytically designed security mechanisms. The authors present a low-cost implementation of a flexible SDN test-bed, specifically focused on security experimentation in respect to security services provided by SDN to both the network and application layer. The test-bed consists of seven switches (annotated S1 to S7), a controller, a server and a typical switch for VPN connection. It can be split into two networks: a control network (connections between the switches and the controller) and a data network (connections between the switches, including the server). There is also a VPN network allowing remote configuration of all test-bed nodes via SSH protocol. All switches use the Ubuntu 16.04 operating system and OpenVSwitch 2.1.1-based (OVS) implementation of OpenFlow protocol in bridge configuration. The test-bed can be also used for the validation of earlier results, obtained analytically or from emulation (e.g., Mininet) and simulation (e.g., ns-3) tools.

Lee et al. [48] proposed a redesigned untraceable Blind Packet Forwarding (BPF) method, based on the Public-key Encryption with Keyword Search for Restricted Testability (PEKS-RT) algorithm, in which the specific host IP address cannot be guessed. The main feature of this approach is that when the source host encrypts the destination host address, it includes the source host's private key, the destination host's public key, and the destination host address as parameters for encryption. Another feature is that the destination host generates the trapdoor value using the destination host address, the source host's public key and the destination host's private key. A centralized SDN controller is used for reducing the overhead of routing data processing of the existing method, increasing this way the operational efficiency. The authors describe a prototype implementation for the blind packet forwarding using PEKS-RT. Their approach is realized in the SDN environment using the Mininet emulator, where Open vSwitch is used as a switch and Floodlight as a controller. The function of the Floodlight controller is expanded to implement the untraceable blind packet forwarding, and it can manage the trapdoor table and control the path using PEKS-RT. Stanford PBC library is used to generate key pairs, trapdoor values and encrypted addresses.

Furthermore, Soule et al. [34] described active defensive deception in the context of distributed systems, and built a prototype that creates an alternate reality in which to trap, learn about, and manipulate adversarial actors without affecting normal and legitimate operations. This prototype, called KAGE, employs SDN and virtualization in order to create a malleable substrate in which deception can occur. The authors demonstrate a preliminary feasibility test of an active deception approach. The test implemented and successfully executed multiple variations of a demonstration scenario that integrates and exercises many of the major KAGE components, in order to orchestrate a brief deception campaign. The demonstration makes use two KAGE plugins: a port scan detector acting as a sensor, and an SQL injection detector adapted to work as both a KAGE sensor and actuator. The distributed nature of KAGEs' building blocks adds complexity, in terms of dynamic distributed composition, and with respect to the timing expectations/challenges regarding interactions with networks, hosts, and services. Furthermore, deviation from expectations can provide indicators to attackers that they are being deceived.

Mishra et al. [38] discuss the Global Environment for Network Innovation (GENI) deployment and research at the US Army Research Laboratory. GENI is a comprehensive test-bed technology to promote rapid network research and application development. It provides sliceable experimental spaces for conducting isolated computational experiment, and supports OpenFlow and other SDN features for conducting comprehensive network research. The Army Research Laboratory (ARL) deploys its own clearinghouse that can act as GENI authority for its own nodes, as well as for all other GENI nodes that come up on the Department of Defense (DOD) network. This customization helps ARL to stand up its node, without delegating its authority to an external entity. Moreover, Jalaian et al. [41] developed a mathematical model in order to realize a unified programmable control plane for heterogeneous wireless networks. The developed framework characterizes the interaction between the physical, link, and network layers for the unified programmable control plane in a heterogeneous wireless network. By applying the framework on a throughput maximization problem, the authors show an application of the model on solving practical issues in a tactical network and gaining some theoretical insights on the optimal behavior of the unified programmable control plane for a heterogeneous wireless network. The authors present numerical results to study the performance of the unified control plane for wireless heterogeneous network. Simulation settings consider a randomly generated multi-hop wireless network with 30 nodes that are distributed in a 100 × 100 area. All units for distance, data rate, bandwidth, and power with appropriate dimensions are normalized, while at the network layer minimum-hop routing is employed. Additionally, Battiati et al. [53] presented a Cyber Security Simulation Service (CSSS) platform, which provides a simulation environment for modeling the impact of cyber-attacks and related countermeasures in tactical networks using SDN. The CSSS integrates a scenario simulator, a network/cyber simulator, a graphical user interface, and a real SDN Controller. Furthermore, the authors showed the functionality of the CSSS in a specific use case, i.e., a black hole attack is performed and the BRAVO (A Black-hole Resilient Ad Hoc on demand distance Vector Routing for tactical communications) approach is utilized as a countermeasure.

Finally, Li et al. [49] presented a hierarchical self-organizing SDN architecture for mobile tactical networks, where the network is dynamically self organized and partitioned into multiple temporary domains, while each domain is assigned with a node that operates as the local SDN controller. A corresponding protocol is proposed by the authors, including (i) a neighborhood discovery mechanism, (ii) a distributed network partition algorithm, and (iii) an abstraction of dynamics. The proposed mechanisms provide strong incentives towards future research and development, although extended verification and proof of concept experiments are recommended.

4.5. Basic Evaluation

Five articles provided a basic evaluation in respect to tactical, military, and naval networks with main focus on the control layer. Athmiya et al. [37] demonstrated and evaluated the implementation of an OpenFlow SDN controller within tactical scenarios, seeking to identify how such implementations can enhance agility, scalability, and network management flexibility for the tactical edge. The article provides a comprehensive presentation of OpenFlow, in terms of overall operation, matching criteria and internal messaging between the controller and the switches. Accordingly, the article briefly describes the Mininet prototyping environment, which is further utilized for the development of an experimental setup, towards verifying the capacity of OpenFlow to satisfy the requirements of the tactical environment. The examined test cases refer to (i) diversion networking, (ii) central policy management for access control lists, and (iii) the distribution of SDN controllers. The article is comprehensive, and promotes further evaluation for providing proof that OpenFlow can be aligned with the requirements of the tactical environment.

Dilmaghani and Kwon [35] proposed an SDN based approach for load balancing within naval military scenarios. The authors construct an experimental setup using Mininet, and utilize Floodlight as the protocol for the communication among switches and the controller. The experimental setup consist of five WAN (Wide Area Network) switches, which correspond to three ships and two on-shore data centers. Furthermore, the scenario assumes three types of traffic with distinct priorities. The article offers a detailed presentation of the evaluation scenario details, while the results highlight the benefits of corresponding SDN implementations, in terms of network programmability and management automation, but also in terms of load balancing and reliability.

Additionally, Anderson [52] described an investigation into five open-source controllers using a specific set of criteria based on the characteristics of these networks. A qualitative investigation compared the controllers based on their state handling and failure recovery mechanisms, and resulted in the selection of two controllers for further investigation. Further quantitative tests were performed on these two controllers, in order to determine which was more suitable for deployment in an airborne environment. Fonger et al. [57] proposed an architecture that serves as a guide for current and future experimentation on trust management and protection in tactical SDN when used with mobile nodes in a coalition operation. However, this work does not discuss thoroughly the security of the information transported through the network, focusing on the protection and separation of different data flows. This separation needs to be robust and reliable, but it does not provide security services on the content of the flows. Finally, Spencer et al. [36] identified the key types of messages used in OpenFlow, and how their overhead is influenced by network characteristics in military networks. Furthermore, the authors presented a series of mitigation measures for reducing or eliminating the overheads, some of which are possible to implement within the current SDN standards, while others require further extensions. The authors perform an experimental validation to quantify and confirm their analysis, where the scenario is implemented using Mininet with OpenVSwitch as the switching element, and netem for performing network simulation.

5. Additional Contributions

In this section, we discuss the articles that have been identified as additional research contributions. These articles do not precisely match the objectives of the review, but discuss closely related topics that can be aligned with military and tactical networks at large, with respect to SDN related technologies. Such examples are Network Function Virtualization (NFV), Wireless sensor networks (WSN), Satellite Networks (SAT), Underwater Acoustic Network (UAN), Unmanned Aerial Vehicles (UAV) and Software Defined Radio (SDR). Figure 1 shows how associated SDN technologies relate to the ISO reference model. SDN in NFV mostly refers to overlay networks above layer 4, but NFV routing can also be enabled on layers 2, 3 and 4. SDR, on the other hand, is mostly referred to as a piece of virtualized radio software running in a virtualized environment. Similarly, we discuss the articles concerning these associated SDN technologies by categorizing them, and summarizing their research contribution, while additional contributions concerning SDN control plane security are also discussed in this section.

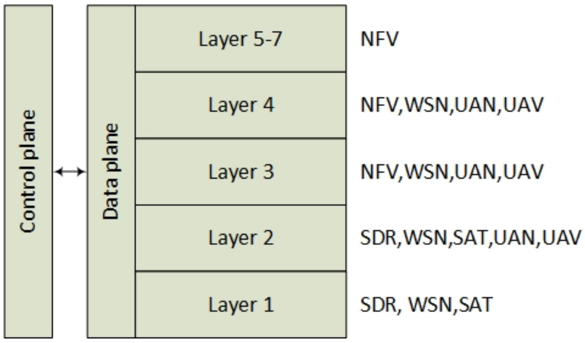

Figure 1. Associated SDN technologies.

5.1. General Software Defined Network Applications

Twenty-six papers [59–84] have been found to discuss SDN applications in a context slightly related to military networks. SDN applications can be used to control network traffic, monitor, test, or orchestrate a network. In military networks running SDN, these applications can simplify both operational and administrative tasks in the network. This includes simplifying the management operations such as applying monitoring to network elements [59], but it can also be used in other contexts such as routing network traffic in power grids on a military base [61], or tracking moving base-stations in vehicles [63]. However, the articles that are reviewed in this sections do not apply directly to the military domain, but include general SDN applications that have been identified by the corresponding authors as adoptable to the military domain. The nature of the SDN technology is appealing to military networks, since SDN offers lower complexity and lower cost that allows for fast failovers and network redundancy in low cost networks, without using expensive technologies such as MultiProtocol Packet Label Switching (MPLS).

SDN opens up for a more flexible routing mechanism, where the network routing on switches and routers can be based on more attributes than only the destination IP and MAC address. This flexible forwarding mechanism applies per flow, and therefore it is possible to use SDN to achieve multipath routing [79]. In military networks, load balancing/ multipathing of constrained bandwidth links is a cheaper alternative than overlay networks or BGP. From a security perspective, multipathing also makes it more difficult to do wiretapping, when parts of the network traffic are diverted around the wiretap. An alternative to physical multipathing is to use multiple radio channels or optical channels to split the traffic into multiple virtual frequency channels [73].

The concept of making advanced routing decisions based on alternative headers other than the IP addresses is also reflected through security and content routing. An approach for confusing an attacker is suggested by Chang [62], by randomizing IP addresses and routing according to other attributes such as the IP option field. However, such SDN routing applications are only possible in small and closed networks. A similar approach also applies to content-based networking (CBN) [70], by extending the network devices to also be able to read the data content of a packet and base the routing decisions on content. Currently, no SDN technology is available for CBN, and no standard exists on how the network packet headers and the data content is used for making routing decisions.

Advanced SDN routing can also be enabled by mixing packet header attributes. In order to enable network isolation, it is most common to use one domain identifier in the packet header, such as a VLAN ID for layer 2. Schlesinger [82] presents an abstraction layer for network programming that opens up for utilizing a combination of both layer 2 and layer 3 when making SDN forwarding rules. This enables network isolation within one VLAN when IP addresses do not overlap.

Monitoring applications combined with flow control in SDN can also increase the performance of an SDN network. Due to the dynamics of SDN, network flows can be specified and changed in a per flow, per network device basis. Hence, the controller is capable of calculating the utilization of the network links and performing load balancing and prioritization of flows per link. By calculating the full paths and their bandwidth utilization, spectral graph theory can be used to increase the robustness and the performance of low bandwidth military networks [71]. A similar network performance enhancing application is also suggested in an architecture named WASP [69] that is customized for wireless networks. It shows that less distributed management traffic across nodes, by replacing distributed protocol with SDN, enhances the overall network performance. Another type of an SDN application is a network testbed. Chadha et al. [60] shows the importance of having testbeds in both civil and military contexts to increase the quality and security of an infrastructure. The author shows how using SDN as a networking tool to create a virtual network infrastructure on a server that is used for quality assurance and testing, in order to ease network provisioning. Accordingly, Ficco et al. [83] demonstrated how OpenFlow in test-beds for military use significantly reducing the costs of testing critical infrastructures.

5.2. SDN Control Plane Resilience and Security

Machuca et al. [81] presented a survey of disaster resilient SDN networks that is transferable to the military context. The survey points out unresolved issues concerning security considerations and disaster scenarios. To overcome the single point of failure (SPoF) of a network controller, multi-controller and multi-domain topologies have been suggested, but, according to the author, this approach introduces a new security problem on the orchestration and management layers. Trends of cloud computing services also apply to military services, where SDN networks with one network controller often are pointed out as a critical part of the infrastructure [74]. Hai et al. [84] suggests an efficient way to overcome the SPoF problem by putting a redundant load balancer in front of a pair of network controllers. However, multi-controller orchestration is not mentioned in the article. A similar approach was also demonstrated by Dilmaghani et al. [35] (see Section 4.5) that presented an SDN load balancing design for naval networks.

In military networks, it is critical to maintain access to network services, especially under disasters and critical operations. The SPoF problem does not only concern the availability and the load on the controller, but it also applies when the network devices do not have network connectivity to the controller. Distributed content caching in vehicles, can assure that information can be distributed to devices around the vehicles if the vehicles lose up-link network connections. Tabata et al. [67] suggests to use many distributed SDN controllers and to alter the OpenFlow rules during online and offline caching operations. The paper demonstrates the concept, but it introduces a security concern due to operating multiple SDN domains that is not mentioned in the article. However, Macedo et al. [80] presents a survey of the relationship between SDR, SDN and NFV and points out security and inter-domain communication of SDN controllers as the main research challenges, something that is also transferable to the military context.

Sorensen et al. [75] showed how SDN in a federated network can enforce network policy control across domain borders in military networks. However, in a multi-domain SDN topology with distributed SDN controllers, the SDN flow rules can come in conflict with each other. In networks such as military networks, security precedence can have higher prioritization than the current OpenFlow specification allows. The authors of an architecture named Brew [64] suggested to extend the OpenFlow specification in order to calculate reconciliations of conflicting SDN rules between controllers. In addition to conflicting rules, the integrity of the rules is also pointed out as a security weakness in multi-domain topologies. This is presented by Beton et al. [72] who is suggesting to use a BGP route reflector with route filtering capabilities based on allocation, reputation and path analysis. SDN with OpenFlow can then contribute to making route filtering policies. However, Porras et al. [76] also show that within a single OpenFlow domain, multiple SDN applications must also meet stringent security requirements. The authors here presented a security framework to handle conflicting SDN rules between different applications. Furthermore, Ahmed et al. [85] focused on mitigating DNS Query-Based DDoS Attacks with machine learning on SDN, and implemented a prototype based on traffic features using Dirichlet process mixture model (DPMM) for clustering traffic applications flow, including those used for DDoS attacks in an unsupervised manner.

Designing a critical infrastructure topology also includes placing network devices strategically, in order to achieve network redundancy and to have backup sites ready when disaster happens. Ashraf et al. [65] suggests utilizing SDN flow-rule parameters combined with monitoring, in order to calculate where it is most efficient to place backup switches to make the network more resilient. Savas et al. [78] suggested a procedure for dynamically setting up a full network on a new site after a disaster, where the use of SDN can accelerate the provisioning time. The procedure includes a recovery provisioning, an upgrade procedure, and a prioritization policy for network resources. Making a resilient SDN network also includes operational management tools to ensure attack protection of the SDN controller. Ionita et al. [66] shows that SDN networks are vulnerable, and that there is a need for additional visual analytics tools for protection against the new threats arising from SDN, such as Denial of Service attacks towards network controllers. Skoin et al. [68] points out a set of physical infrastructure attacks such as wiretapping, electromagnetic pulses (EMP), and critical hub nodes "take-out". The author suggest that centralization of network controllers in OpenFlow introduces new vulnerabilities and makes security even more complex. Correspondingly, Dahan et al. [77] pinpoint that the network controllers must be both secured from passive and active attacks, as well as physical and network attacks.

5.3. Network Function Virtualization

Network Function Virtualization (NFV) refers to the concept of moving network services into a cloud environment. A characteristic networking feature in NFV is Service Function Chaining (SFC) that enforces end-user data traffic to traverse data-center services also known as middleboxes. SDN is a technology that can be used to enable such routing, where the SDN controller is responsible for steering the traffic through a chain of such NFV services. Eight articles have been found to discuss NFV in a military context [86–93].

An NFV and SDN survey by Cox et al. [86] presents both civil and military application domains by coupling NFV with SDN. Content-centric networking, on-demand virtual networks, and cloud services are examples of how NFV can contribute to make a more reliable, faster and secure network. NFV contributes to solve the multi-domain SDN controller problem by abstracting the inter-domain communication to a standardized NFV orchestration level. However, orchestration, interoperability, portability, integration, management, automation and resiliency are new research challenges that must be solved.

Rametta et al. [87] presents an architecture of how drones can transmit video in rural areas with the support of an NFV/SDN enabled backbone. This is an example of a military application in a distributed NFV topology, where distributed Virtual Network Functions (VNFs) are used as distributed video storage and network overlay routing. By re-encoding video, the distributed NFV services can then adapt the video quality based on bandwidth constraints, while Service Function Chains (SFC) can be used in order to select the most appropriate network path. A similar overlay network application is suggested by Li et al. [88], where distributed NFV services are used in order to route the network traffic based on an overlay network with SFCs instead of plain destination IP routing. Distributed QoS algorithms can then ensure QoS in the overlay network, based on bandwidth requirements and policies. Their results are also reflected through a paper of satellite SDN networks [90], a survey [89] of NFV in military networks and an NFV-based satellite architecture of distributed NFV.

All authors state that distributed NFV is a new way to distribute routing, enable security policies by overlay networks, and increase network performance. Shi et al. [91] also presents challenges with the management and orchestration of such typologies in the context of space-ground networks and cross-domain applications. However, all the papers suggest future work to be focused around the orchestration of the NFV services, and how to translate the security policies across the domain boundaries. It is noted that none of the reviewed papers discuss or give an example of control plane to control plane protocols of the overlay NFV networks in a military context. This corresponds to the NFV approach of using the orchestration layer for inter-domain communication. However, Carey et al. [93] suggests an SDN approach for an inter-domain control plane protocol, in order to increase the performance in heterogeneous military networks. They indicate that the use of API based control plane to control plane communication is enhancing the network performance compared with traditional BGP communication.

5.4. Software Defined Satellite Network Applications

Future military space operations are expected to become more complex and operate further from Earth. Hence, there is a need for autonomous networks that can configure themselves with minimal human intervention. Automation through SDN principles is a promising technology for overcoming this need. A survey of satellite communication systems by Radhakrishnan et al. [94] states that, for the OSI layer 1, Software Defined Radio (SDR) is expected to enable radio frequency sharing jamming detection, while traditional SDN enables flexible routing based on layers 2 and 3. Two papers have been found that discuss SDR in the satellite context [95,96], while SDR is further discussed in Section 5.6.

Operationally Responsive Space (ORS) is a satellite technology defined by the US Department of Defense. It is suggested to base the network on SDN, but only two papers concerning the military application domain and Software Defined satellite Networks have been found in the literature review. The two research challenges that are pointed out are orchestration and available resources. SDN in space differs from ground SDN, due to the distinct mobility patterns, and the fact that satellites can come out of reach due to their mobility patterns. However, their location can be predicted if they come out of reach [97]. Hence, an abstract network model is needed, in order to make an application that can make such predictions. Space networks have a long transport delay and limited resources that result in a flow table management problem. Hence, making small SDN flow tables is preferable, without having too many table-misses. Li et al. [98] suggested an algorithm to balance flow table size and table misses, but does not discuss any security implications about reducing the table size.

5.5. Software Defined Wireless Sensor Network

Modieginyane et al. [99] highlighted application challenges faced by WSNs for monitored environments, as well as opportunities that can be realized on applications of WSNs using SDN.

The authors also proposed a method of implementing simple state rules on the sink node, as an effort to improve the Software Defined Wireless Sensor Network (SDWSN) programmability, as well as to offload the controller of such low-level computational tasks. Aleksander et al. [100] presented a model that uses SDN in Wireless Sensor Networks. Wenxiang et al. [101,102] studied a model and method for applying SDN to Wireless Sensor and Actor Networks (WSAN), with the objective of improving communication efficiency and expandability. The detailed model includes a three-layer architecture with a new control plane, relevant system entities, and enhanced protocol stack for cooperative communication and task execution. Furthermore, the authors explored the challenges and mechanisms for effective system management for aspects related to mobility, security, heterogeneity, topology construction and controlling the load of the SDN controllers. Kahjogh et al. [103] presented a novel approach utilizing a Mixed Integer Programming (MIP) optimization to extend network lifetime and reduce latency in WSNs. The authors also explained how such an approach is made viable for WSNs via new wireless SDN architectures and protocols.

Furthermore, survey papers on general SDWSN aspects and requirements have been identified [99,104]. Ndiaye et al. [104] highlighted work on traditional WSN management, and reviewed SDN-based techniques for WSNs in detail, while focusing on the advantages that SDN offers. Furthermore, the authors discussed open research challenges across mechanisms for SDN-based WSN configuration and management. Modieginyane et al. [99] highlighted application challenges faced by WSNs for monitored environments, as well as opportunities that can be realized on applications of WSNs using SDN. The authors also proposed a method of implementing simple state rules on the sink node, as an effort to improve the SDWSN programmability, as well as to offload the controller of such low-level computational tasks. Furthermore, Aleksander et al. [100] presented a model that uses SDN in Wireless Sensor Networks.

Other research directions in the area of SDWSN include software defined mobile sensor networks [105], software-defined sensor networks [106,107], resource optimization using SDN for smart grid WSN [108], SDN based QoS provisioning in WSN technologies [109], and others [110]. Yuan et al. [105] introduced a novel mobile sensor networking architecture for a swarm of micro unmanned vehicles (MAVs) using SDN technologies. Additionally, the proposed networking architecture provides potential applications for advanced routing policies for a swarm of MAVs with highly dynamic topologies. Sayyed et al. [108] discussed the concept of SDN in WNS where OpenFlow is the controller part of the network. Letswamotse et al. [105] proposed improving QoS provisioning by introducing SDN principles into WSN technologies, while Zeng et al. [107] considered a minimum-power activation and scheduling problem in multi-task SDSNs with quality-of-sensing guarantee. The authors derived the effective sensing rate that can be achieved by collaborative sensing from multiple sensors in closed-form. Zeng et al. [106] introduced the concept of SDSNs and outline several pioneering related work and enabling technologies for the realization of SDSNs. Furthermore, Fortino et al. [111] identified motivations and challenges for the integration of body area networks (BANs) and Cloud computing. The authors presented a general reference architecture, based on purposely elicited requirements for supporting cloud-assisted BANs, from sensor data collection to workflow-oriented data analysis: (1) sensor stream efficient collection, (2) effective sensor stream management, (3) scalable sensor stream processing framework, (4) persistent sensor data storage, (5) workflow-oriented decision making, (6) advanced visualization services, and (7) multi-layer security. Finally, Junli et al. [112] designed an efficient energy routing algorithm based on SDWSN, where the algorithm is operated in a controller that establishes distance queue, based on the information collected from the nodes, and computes the closest node to transmit data.

SDN is also used in the Internet of Things [113–116]. Gonzalez et al. [113] presented their preliminary study that is focused on the understanding of an effective approach to build a cluster network using SDN. The proposed approach is a new method for a new type of IoT network based on SDN in cluster environments. The system is able to handle the communications between clusters by means of an SDN cluster head, managed by an SDN controller. Tortonesi et al. [116] presented an

SDN-based middleware solution to mitigate the IoT information explosion. Abels et al. [110] discussed future proof IoT concepts including composable semantics, security, QoS, reliability, and software defined IoT (SD-IoT) that controls and updates for any hardware, anywhere, anytime, including edge and WSN. Ionita et al. [114] proposed an infrastructure based on custom locally installed agents which communicate with a central AlienVault deployment for event correlation. The agents are based on a neural network which takes actions based on a risk assessment inspired by the human immune system. The proposed implementation can successfully be implemented in an IoT scenario, with added security for the "brownfiled" devices. Singh et al. [115] proposed a semantic Edge based network model, which plays a significant role for communicating tactical and non-tactical pieces of information over the network. Furthermore, the exchange of information and subsequent data analysis on the military health service (MHS) makes the system intelligent.

5.6. Software Defined Radio

Moy et al. [117] discussed Software Defined Radio, emphasizing the fact that SDR is a major evolution of radio technologies, and a convergence of different pre-existing fields. Ulversoy [118] discussed SDR challenges and opportunities, while Kacpura et al. [119] presented SDR architecture contributions for next generation space communications. Sigholm et al. [120] presented a best-effort approach to Data Leakage Prevention (DLP) for inter-organizational Re-configurable Radio Systems (RRS)-based networks. The proposed architecture makes use of data mining techniques, and an efficient n-dimensional clustering algorithm which has previously been successfully used for real-time anomaly detection in critical infrastructure protection. Cormier et al. [121] explored automated, dynamic large-scale radio reconfiguration, through the implementation and characterization of three alternative re-configurable radio designs. These implementations seek to quantify the impacts of implementing large-scale radio re-configuration through SDR application management, enabled by SDR architectures. Androlewicz et al. [122] presented selected research activities at the Air Force Research Laboratory's Space Vehicles Directorate (AFRL/RV), in the arena of software-defined and cognitive radio technology for military space-based applications. Current efforts include development of SDR controlled satellite ground-stations, networked ground station operations for increased efficiency, as well as research into new radio control algorithms and methods of dynamic waveform reconfiguration for satellite applications. Moessner et al. [123] focused on ubiquitous wireless network accessibility, and described the necessary research directions for advancing the SDR technology as a facilitator of ubiquitous access.

SDR is used in different applications. Noble et al. [124] described a methodology for jamming traditional combat net radios using commercial SDR mounted on unmanned aerial vehicles, while the authors proposed tactics, techniques, and procedures for employing this system within an infantry battalion. North [125] explained recent changes to the JTRS (Joint Tactical Radio System) program, and its new approach to delivering wireless networking capabilities to the warfighter. All JTRS products are based on SDR technologies, in order to enable a more scalable and extensible radio system in comparison to a system composed of dedicated hardware. Wei et al. [126] investigated received signal strength indicator (RSSI) based localization, which attracts a lot of interest because of its simplicity. In order to improve the performance of RSSI based localization, the authors proposed a bias reduction algorithm. Wang et al. [127] described the networking usage requirements for MANET over legacy narrowband tactical waveforms. First, the authors discussed the common characteristics of legacy tactical radio waveforms and the implications of such characteristics for the MANET implementation. Then, an actual MANET implementation over a legacy tactical radio waveform on an SDR is presented with the results of actual field tests.

Almoualem [128] presented a resilient wireless communication architecture based on Moving Target Defense (MTD), and Software Defined Radios (SDRs). The approach achieves resilient operation by randomly changing the runtime characteristics of the wireless communications channels between different wireless nodes, aiming to make it extremely difficult to successfully launching attacks. Enrico et al. [129] overviewed the NATO initiative to develop tactical waveform specifications for VHF and UHF communications that are free of intellectual property. These waveforms are for multinational interoperability between NATO nations and coalition users, and can be implemented on SDR platforms in tactical radios. The security architecture has been included in the design from the beginning, and the performance is targeted to be vastly improved over legacy waveforms.

Other research efforts of SDR are presented in [130–135]. Kaur et al. [132] discussed SDR and different routing protocols for MANET. The MANET Reactive protocol (i.e., AODV) is implemented for SDR by using CSMA/CA, with some modifications. Singh et al. [130] provided a review of the motivation, workflow and results of the NATO Research and Technology Organization (RTO)/Information Systems Technology (IST) Research Task Group (RTG) on SDR, which works on the issues concerning Software Communications Architecture (SCA) based implementations of waveforms on SDRs. The authors presented the SCA-based implementation results of STANAG 4285 waveform, and the effect of increasing the granularity of the SCA waveform application on the system overhead. Mahasamudram et al. [133] envisioned that the Agile Cognizant Transceiver (ACT) platform built helps faster prototyping of defence systems and paves the way for faster product induction cycles in defence automation. ACT is a complete indigenous solution developed with SDR, in order to support wide band requirements and multi technology waveforms. Moura et al. [135] presented case studies of attacks aimed at tactical SDR, based on a classification with the most common sources of vulnerabilities, classes of attacks, and types of intrusions that military radio sets may suffer. The authors also described how attack mitigation strategies can impact the development of SDR infrastructures.

Amjad et al. [136] presented a comprehensive survey of full-duplex (FD)-cognitive radio networks (CRNs) communication. The authors covered the supporting network architectures and the various antenna designs. The authors also surveyed major advances in full-duplex medium access protocol (FD-MAC) protocols as well as open issues, challenges, and future research directions to support the FD operation in CRNs. Chandrasekharan et al. [137] reported the detailed account of the design and implementation challenges of an aerial network consisting of LTE-Advanced (LTE-A) base stations. In particular, the authors reviewed achievements and innovations harnessed by an aerial network composed of Helikite platforms. Helikites can be raised in the sky, while they carry battery, antenna, and RRH (Remote Radio Head) equipment to bring Internet access during special events and in the aftermath of an emergency. Cao et al. [138] described the rapid development of a P25 waveform on a surrogate Joint Tactical Radio System (JTRS) SDR platform. The JTRS program is enabling communications within the military, by implementing different military radio waveforms on SDR platforms. Furthermore, the authors presented the design and implementation of a three way voice bridge among P25, the future multiband multiwaveform modular tactical radio (FM3TR), and Voice over Internet Protocol (VoIP), with software communication architecture (SCA) compliant implementation for both the P25 and FM3TR waveforms. Favraud et al. [139] surveyed possible public safety use cases with the induced network topologies, discussed the current status of the 3GPP standards, and highlighted future challenges. The authors further elaborated on the need to support mobile backhauling in moving-cell scenarios, and describe two LTE-based solutions to enable dynamic meshing among the base stations.

Lal et al. [140] surveyed the existing security attacks along with their state-of-the-art countermeasures and respective limitations. The authors also proposed new security paradigms for detecting and counteracting malicious activities, both from a generic perspective and within specific scenarios in Underwater Acoustic Networks (UANs). The main research challenges related to the cooperation of mobile and static nodes in a distributed and ad hoc way have been addressed, together with the investigation of multi-metric accurate reputation systems, secure deployment and adaptive monitoring techniques. Baldini et al. [141] discussed a range of issues that have been identified thus far within the European Commission Seventh Framework Programme project known as EULER, which seeks to demonstrate the benefits of software defined radio technology to support the resolution of natural disasters of significant stature. In particular, the perceived pan-European interoperability of public safety, and coordination with military devices and networks. Aspects of interoperability are also extended to the three dimensions of platform, waveform, and information assurance. Adrat et al. [142] analyzed if an added value can be provided to the operators, by SDRs hosting an "enhanced" legacy waveform, where this is introduced in a way that guarantees the interoperability with the legacy equipment. While the legacy waveform acts as base-layer, some enhancement-layers offer an extra budget for the transmission of additional information. This spare budget can be exploited in order to increase the data rate (i.e., throughput), the error robustness (and with this communication range), or both. Bader et al. [143] presented mobile ad hoc networks in latency-and bandwidth-demanding mission-critical applications, while the authors analyzed and validated efficient and low-complexity remedies to those issues, and validated their results based on field experiments carried out using SDR platforms. Compared with the classical Mobile ad hoc network (MANET) routing schemes, autonomous cooperative routing (ACR) was shown to offer up to two times better throughput and more than four times reduction in end-to-end latency. Finally, Bor-Yaliniz et al. [144] studied the opportunistic utilization of low-altitude unmanned aerial platforms equipped with base stations (i.e., drone-BSs) in future wireless networks. In particular, the authors envisioned a multi-tier drone-cell network complementing the terrestrial HetNets. Furthermore, they investigated the advancements promised by drone-cells, and discussed the challenges associated with their operation and management.

5.7. Unmanned Aerial Vehicles' Applications

A survey of Gupta et al. [23] focused on the research potential of Unmanned Aerial Vehicles (UAV), where SDN can contribute to lowering cost and increasing availability in both public and military UAVs. The UAV networks need to support dynamic nodes with frequent change of network topologies, where nodes have a high network outage rate. Due to the need for OpenFlow network controller availability in dynamic networks, this requires a distribution of network controllers where balance and cooperation between network controllers must be addressed. However, the authors state that hybrid SDN with delegated packet processing is the most promising SDN technology for UAV. The current protocols for network routing in UAV have high latency, while the fast, flexible routing and multipath selection in SDN are assumed to out-perform current UAV routing protocols. Correspondingly, Mahmoud et al. [145] presented an architecture based on SDN, where UAV sensors controlled by OpenFlow are expected to increase reusability, scalability and modularity in the UAV network. The UAV papers refer to hardware security, management and orchestration as research challenges.

5.8. Underwater Acoustic Networks Applications

Underwater acoustic networking (UAN) is a technology that enables new SDN applications for both commercial and military use. This includes underwater surveillance and data collection of ocean characteristics. Normally, the acoustic channel for underwater communication is characterized by noise, multipath, delay and path loss, while SDN can enable a more intelligent routing mechanism in such environments. This is reflected by two UAN papers [146,147] that adopt the principles from OpenFlow to underwater networks. The authors present two examples of SDN architectures in order to achieve a more flexible routing, based on OpenFlow principles in the UAN domain. Demirros et al. [148] also emphasized the need for low energy consuming sensors and presented an architecture of an underwater sensor network with hardware sensors running on a hardware chip with customized SDN software.

6. Statistical Analysis and Metrics

This section presents a statistical analysis of the reviewed articles. All articles have been sorted and categorized in respect of authors, affiliations, citations, publication attributes and their relation to SDN technologies. The articles are also divided into significant research contributions and additional research contributions. This is reflected through the previous sections and summarized here.

6.1. Type of Publication

Table 2 shows the distribution of the types of articles. In total, 134 reviews were conducted, with 51 journal articles, 78 conference papers and five other types of contributions. Ten of the journal papers and 31 of the conference papers were identified as articles with significant research contributions (Section 4), while 30 of the journal papers were published in an IEEE journal, and all other journal papers had no significant channel commonalities. Out of the conference papers the Military Communications Conference (MILCOM), the International Conference on Military Communications and Information Systems (ICMCIS) and the Military Communications and Information Systems Conference (MilCIS) were the only common conferences with more than one contribution within the field of military SDN (Table 3). This indicates that the relevant work within the topic is mostly presented at military oriented conferences. All of these military conferences were published with IEEE. For all other articles, IEEE also clearly contributes with the most publications related to military SDN, as our literature search found 74.6% of all articles to be published by IEEE (Table 4). It is noted that no PhD thesis was considered to fit the military application domain, while 20% of the extracted articles originate from institutions directly connected to the military.

Table 2. Type of articles.

Type of Article	Significant Contributions	Additional Contributions
Journal	10	41
Conference	31	47
Master Thesis	2	1
PhD Thesis	0	0
TechReport	0	2

Table 3. Top conferences.

Type of Article	Significant Contributions	Additional Contributions
MILCOM	10	9
ICMCIS	6	0
MILCIS	3	0
Other	12	38

Table 4. Top publishers.

Type of Article	Significant Contributions	Additional Contributions
IEEE	35	65
Elsevier	0	5
Springer	0	5
ACM	0	2
Other	8	14

6.2. Author and Affiliation Contribution

In this subsection, statistical information about the authors and their affiliations are summarized, both for the significant and additional research contributions. Tables 5 and 6 present the distribution of authors and affiliations among the selected articles. Only the affiliation of the main author is counted in respect to the affiliations (Table 6), while all contributing authors are taken into account for the metrics related to the authors (Table 5).

A correlation is visible between the most contributing authors and their affiliations, meaning that it is the authors and not the affiliations that contribute primarily to the ranking of the affiliations. The University of California, Hague University and the US Army have the most contributing authors for military SDN related articles, while these authors also contributed to common articles. From an SDN categorization perspective, the affiliations have no clear contribution within any subtopic of military SDN. Within the different research fields of military SDN, the University of Wuhan contributes the most within Wireless Sensor Networks, while Colombia University contributes the most within Unmanned Aerial Vehicles. Furthermore, for research contributions within SDN security applications, the US Army and Hague University rank as the most significant contributors.

Table 5. Author contributions.

Number	Author	Article
5	Wrona, Konrad	[29,30,39,42,44]
4	Gerla, Mario	[15,45,56,147]
4	Mishra, Vinod	[28,38,40,42]
4	Spencer, Jon	[21,36,42,46]
3	Hancock, Robert	[36,42,46]
3	Williams, Christopher	[28,31,40]
2	Abu-Mahfouz, Ad.	[99,104]
2	Adrat, M	[130,142]
2	Amanowicz, Marek	[30,44]
2	Bouet, Mathieu	[18,33]
2	Dasari, Venkat	[38,41]
2	Du, Pengyuan	[45,56]
2	Fernandes, Ricardo	[16,54]
2	Gaspary, Luciano	[16,54]
2	Hoffmann, Ceilid	[45,56]
2	Ionita, Mihai-Gabriel	[66,114]
2	Kohl, Anderson	[16,54]
2	Letswamotse, Babedi	[99,109]
2	Luo, Hongbin	[88,98]
2	Malekian, Reza	[99,109]
2	Miyazaki, Toshiaki	[106,107]
2	Modieginyane, Kgotla.	[99,109]
2	Moy, Christophe	[117,141]
2	Oudkerk, Sander	[30,39]
2	Patriciu, Victor-V	[66,114]
2	Pezaros, Dimitrios	[19,81]
2	Phemius, Kévin	[18,33]
2	Stocchero, Jorgito	[16,54]
2	Sturman, Taj	[96,141]
2	Szwaczyk, Sebastian	[30,44]
2	Verma, Dinesh	[28,40]
2	Wang, Xiang	[51,89]
2	Webb, MichaelR	[17,24]
2	Zeng, Deze	[106,107]
2	Zhou, Huachun	[88,98]

Table 6. Affiliation contributions.

Number	Affiliation	Paper
5	Uni. of California, USA	[45,56,71,78,138]
4	Hague Uni., Netherlands	[30,39,44,129]
4	US Army	[31,38,40,60]
3	Uni. of Pretoria, S. Africa	[99,104,109]
3	Wiltshire College, UK	[21,36,46]
3	Wuhan Uni., China	[101,102,107]
3	Thales, France	[18,33,42]
3	Uni. of Arizona, USA	[64,74,128]
2	Bangalore Uni., India	[37,133]
2	The MITRE Corporation, Bedford, USA	[52,58]
2	Uni. of Bucarest, Romania	[66,114]
2	Uni. of Cambridge, USA	[34,93]
2	Uni. of Jinan, China	[35,126]
2	Uni. of Oregon, USA	[20,110]

6.3. Citations and Publication Year

All reviewed articles were organized with respect to the year of publication. Table 7 shows that most of the significant articles within military SDN are published after 2015. The year of publication table shows an exponential growth of articles for the last four years. It is not clearly known why there is a drop in the number of articles for 2017, but this can be attributed to the time of the literature review and a possible delay in publishing processes. However, the increasing number of articles indicates the relevance and requirements for a systematic literature review on the topic.

Table 7. Year of publication.

Year	Number of Publications
2018	4 (Until 23 August 2018)
2017	34
2016	39
2015	24
2014	17
2013	2
2012	2
2011	3
2010	4
–2009	5

Registered citations from Google Scholar were used as the data source for the number of citations. The distribution of the number of citations (Table 8) shows that the number of the most cited articles is low for the significant articles. This also reflects the increase in significant research contributions in recent years and indicates that the reason for a low citation number can be due to the publication year. Accordingly, it becomes clear that an initial knowledge base has already been established in the field, allowing for crucial contributions to emerge.

Table 8. Number of citations.

Citations	Significant Contributions	Additional Contributions
0	13	13
1–2	13	14
3–4	12	16
5–9	5	13
10–14	0	9
15–29	0	8
30–49	0	10
50–99	0	5
100+	0	3

Tables 9 and 10 show the most cited articles collected in the review. It is noted that the significant research contributions concern primarily SDN in wireless and mobile networks (Table 10). Furthermore, the additional research contributions also relate mostly to wireless technologies, potentially indicating a lack of research contributions on military network control applications with SDN.

Table 9. Top five citations' significant contributions.

Rank	Article	Citations
1	Toward software-defined battlefield networking [15]	8
2	Enhancing wireless communications with software defined networking [17]	6
3	Distributed SDN for Mission-Critical Networks [33]	6
4	Distributed flow controller for mobile ad hoc networks [32]	6
5	Software Defined naval network for satellite communications (SDN-SAT) [45]	5

Table 10. Top five citations for additional contributions.

Rank	Article	Citations
1	Software Defined Radio Challenges and Opportunities [118]	241
3	Survey of Important Issues in UAV Communication Networks [23]	215
2	Securing the Software Defined Network Control Layer [76]	116
4	The New Frontier in RAN Heterogeneity Multi-Tier Drone-Cells [144]	98
5	Designing and implementing future aerial communication networks [137]	90

6.4. Categorization of Software Defined Network Applications

This section summarizes the categories of SDN that have been discussed through this systematic literature review. Section 5 presented additional SDN research contributions that discussed related SDN technologies such as Network Function Virtualization (NFV), Wireless sensor networks (WSN), Satellite Networks (SAT), Underwater Acoustic Networks (UAN), Unmanned Aerial Vehicles (UAV) and Software Defined Radio (SDR). These are mostly related to the application domains of Software Defined Network (SDN) applications and controls. Table 11 reflects the focus of research trends, where the significant research contributions for military SDN are not focused on the related SDN technologies, but mostly on SDN control plane applications.

Table 11. Type of articles.

Category	Significant Contributions	Additional Contributions
SDN	38	28
NFV	0	8
SAT	2	5
UAN	0	3
UAV	2	2
WSN	0	17
SDR	1	28

7. Discussion and Recommendations for Future Work

Although SDN appears to have many potential benefits for tactical military networks, including rapid reconfigurability and improved network situational awareness, it faces certain challenges that could hinder its performance and implementation in tactical military networks [40]. In particular, the low bandwidth and unreliability that characterize military communication links necessitate a highly resilient control plane, and the exposure of the control plane on the wireless medium presents new attack vectors. In the following subsections, we discuss directions for future research covering SDN architecture, controller, services, tools, and basic evaluation in tactical military networks.

7.1. Architecture

Most of the proposed SDN architectures in tactical military networks follow the key ideas of the SDN paradigm. For instance, the SDBN architecture considers four planes: forwarding, control, application, and management [15]. However, the current realizations of SDN technologies are still far from fully addressing the realistic requirements and constraints of dynamic tactical networks, and in extending military networks. Many challenges in SDN architectures require further research effort, with the main focus areas for future research being:

- Development of prototype for East–West communication between network controllers and nations. In the case of a multi-controller-based architecture, the East–West interface protocol manages interactions between the various controllers.
- Resilience of network controllers as they currently present a single point of failure.

- Standardization of Northbound and Southbound interfaces to the SDN controller. The Northbound and Southbound interfaces are currently poorly defined, presenting a barrier to integration with management systems and peer-level networks.
- Data offloading techniques at the physical layer in order to reduce delay and congestion of the network.
- Mechanisms to migrate the SDN controller between nodes connected by restricted bandwidth wireless links.
- Control of network polices and how to share network policies across nations and network controllers.
- Exposure of the control plane traffic over wireless media introduce security vulnerabilities.
- Development of a suite of protocols and applications specifically designed for SDN architectures in tactical, and in extend military networks.
- Targeted study on the functions of SDN that can guarantee the routing QoS for specific operational groups, according to the urgency level of the task, and the scalability of the controller, extending to switches that can be applied to large scale networks.
- Development and testing an architecture dedicated to heterogeneous networks.
- Development of sophisticated schemes for ingress/egress filtering at each real-time SDN-enabled switch. This can help to better identify the properties of each flow (priority, class, delay, etc.) and then develop scheduling algorithms to meet their requirements.
- Enhancement of the SDN paradigm on battlefield networking (SDBN) architecture and the operational scenarios in which the architecture could be deployed. For example, the utilization of high-level policies to operate the SDBN as a whole, could be addressed by intent-based management (i.e., Autonomic Management) or service abstractions for policies (i.e., Simplified Use of Policy Abstractions—SUPA).

7.2. Control Systems

The traditional SDN architecture requires a node to contact the centralized SDN controller whenever it encounters a new request in which it needs to make a decision for a data plane operation, and for which it does not have the required control plane information. However, this centralized architecture is not suitable for military tactical networks with high levels of dynamism and frequent network failures that can result in slow network updates as well as significant controller overhead. The areas for further exploration include, but are not limited to:

- Investigating SDN controller fail-over mechanisms to automatically take the control of the switches when a neighbour controller fails.
- Describing a distributed SDN controller network architecture that can meet reliability requirements through the use of multiple remote SDN controllers with integrated redundancy features.
- Exploring Software Defined Coalitions (SDCs) which share assets at increasing granularity, allowing a better sharing of the network, storage and application level services available in each of the partners.
- Identifying the required and appropriate abstractions which should be exposed to the partners, in respect to the policies of the coalition members.
- Creating the right interfaces for OODA (Observe, Orient, Decide and Act) based control of individual elements.
- Developing appropriate routing, security, information and asset sharing mechanisms for coalition operations.
- Optimizing the policy constructs for coalition missions.

- Defining the interaction between controllers of different nations across interoperability points of a Protected Core (PCore).
- Developing approaches to distribute control where necessary—for example, at the level of individual network functions such as mobility—without sacrificing the benefits of programmability that come from centralization in other areas.
- Examining fault types beyond SDN controller faults, e.g., attacks that aim to exhaust resources in typical SDN switches, with resulting delays in the packet forwarding.
- Recovering from faults using SDN. It is interesting to study whether and how SDN may help speed up recovery from faults in a communication network that supports tactical military networks.

7.3. Tools

Validation and evaluation of performance, resilience and security solutions for complex systems like military networks remain difficult problems. Simulators, emulation platforms and test-beds are useful for proving the efficiency and feasibility of new network architectures/designs and algorithms, and evaluate their capability to address specific challenges of military networks. Future research directions include:

- Designing experiments to study SDN-enabled multi-domain heterogeneous networks, non-IP protocol innovations, and building SDN network exchange (SDX) to act as policy based SDN network peering point for connecting various SDN network prefixes.
- Simulating/experimenting developed mathematical models for realizing a unified programmable control plane, with support of a realistic number of nodes for wireless heterogeneous network.
- Testing the content-based security concept in network exchange points such as Software Defined Exchange.
- Examining the performance of operational aspects of Software Defined Coalitions (SDC) in an emulated test-bed.
- Implementing an operational military Network with SDN where management links are suffering from variances.
- Implementing an operational military Network by including third-party platforms such as Pyretic to the applications code, in order to explore the advantages of the policy enforcement approach.
- Conducting experimentation on an at-scale real SDN testbed for large-scale military networks.
- Extending the testbed setups to be able to demonstrate enforcement of security policies in respect to all three dimensions of security goals, i.e., confidentiality, integrity and availability, and performing experiments involving a combination of cross-layer and network-specific (e.g., network intrusion detection mechanisms)

7.4. Service

Traditional networks are designed for static environments with cabled connections, hence there are some challenges when deploying IP networks in dynamic military operations. To cope with some of the challenges, Tactical Communications (TACOMS) have defined a set of services; two services which solve similar task but have different dependencies are the Autoconnectivity and Service Announcement (SA) and Border Gateway Protocol (BGP) service. Federated Networking Service Engine (FNSE) is a more generic approach for adding network services to NATOs Federated Mission Network (FMN) [25]; however, there are still many areas that require further invstigation, these include:

- Evaluation of alternative East–West protocols;
- How to add anonymity to the authentication phase;
- Measurements of the overhead for secure channel establishment;
- Investigation of how management across Autonomous System (AS) borders can be achieved.

7.5. Basic Evaluation

Software-defined networking has the potential to offer significant advantages over conventional networks in military networks. However, there are still open issues that need to be evaluated before usage in a production environment:

- Evaluation of the SDN control plane performance in large-scale heterogeneous networks, and its ability to respond to failures;
- Evaluation/investigation of the number and placement of controllers. A centralized management miles away from the forwarding devices in an operational scenario is challenging, and the number and placement of controllers is a research problem in military networks;
- Evaluation of extensions to OpenFlow that include features for fine-grained control of wireless access points in a similar manner to OpenRadio;
- Development of a comprehensive methodology to evaluate the performance of SDN load balancers.

8. Conclusions and Limitations

Our objectives with this systematic literature review have been (Step 1: Section 3):

1. To identify and classify the research papers published on the topic of military SDN *(Addressed in Sections 4 and 5)*;
2. To analyze and evaluate the research papers published on the topic of military SDN and summarize the related research results *(Addressed in Sections 4 and 5)*;
3. To identify the most active and influential researchers, groups, conferences, and journals, on military SDN *(Addressed in Section 6)*;
4. To identify the current main focus areas within the topic of military SDN *(Addressed in Sections 4 and 5)*;
5. To make recommendations for future research *(Addressed in Section 7)*.

The initial literature search provided a total of 927 articles, which have been filtered in accordance with their relevance with the investigated topic down to 134 articles. Accordingly, the quality appraisal phase allowed the extraction of 43 articles with significant and targeted research contributions, while 91 more articles have been identified to be highly relevant to the scope of this review (Steps 3, 4 and 5: Section 3). Furthermore, the data extraction and synthesis steps allowed us to reach the aforementioned objectives (Steps 6 and 7: Section 3), as presented in the corresponding sections. According to the findings of our analysis, it becomes apparent that there is a community of interest within the field of military SDN, while many topics within this area remain largely unexplored. Furthermore, these seem to exist a consensus within the community, in respect to the maturity levels of the distinct focus areas, and that the expected benefits from applying SDN within military networks justify the intensification of research effort in the future.

Author Contributions: The authors contributed equally to this work.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Horvath, R.; Nedbal, D.; Stieninger, M. A Literature Review on Challenges and Effects of Software Defined Networking. *Procedia Comput. Sci.* **2015**, *64*, 552–561. [CrossRef]
2. Govindarajan, K.; Meng, K.C.; Ong, H. A literature review on Software-Defined Networking (SDN) research topics, challenges and solutions. In Proceedings of the 2013 Fifth International Conference on Advanced Computing (ICoAC), Chennai, India, 18–20 December 2013; pp. 293–299. [CrossRef]

3. Xia, W.; Wen, Y.; Foh, C.H.; Niyato, D.; Xie, H. A Survey on Software-Defined Networking. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 27–51. [CrossRef]
4. Alsmadi, I.M.; AlAzzam, I.; Akour, M. A Systematic Literature Review on Software-Defined Networking. In *Information Fusion for Cyber-Security Analytics*; Springer International Publishing: Cham, Switzerlan, 2017; pp. 333–369.
5. Kreutz, D.; Ramos, F.M.V.; Verassimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-Defined Networking: A Comprehensive Survey. *Proc. IEEE* **2015**, *103*, 14–76. [CrossRef]
6. Jammal, M.; Singh, T.; Shami, A.; Asal, R.; Li, Y. Software defined networking: State of the art and research challenges. *Comput. Netw.* **2014**, *72*, 74–98. [CrossRef]
7. Lopes, F.A.; Santos, M.; Fidalgo, R.; Fernandes, S. A Software Engineering Perspective on SDN Programmability. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1255–1272. [CrossRef]
8. Goel, N.; Gupta, A.; Singh, S.N. A study report on virtualization technique. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016; pp. 1250–1255. [CrossRef]
9. Jarraya, Y.; Madi, T.; Debbabi, M. A Survey and a Layered Taxonomy of Software-Defined Networking. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1955–1980. [CrossRef]
10. Nunes, B.A.A.; Mendonca, M.; Nguyen, X.N.; Obraczka, K.; Turletti, T. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1617–1634. [CrossRef]
11. Da Silva, R.B.; Mota, E.S. A Survey on Approaches to Reduce BGP Interdomain Routing Convergence Delay on the Internet. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2949–2984. [CrossRef]
12. Hu, F.; Hao, Q.; Bao, K. A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 2181–2206. [CrossRef]
13. Da Silva, A.S.; Smith, P.; Mauthe, A.; Schaeffer-Filho, A. Resilience support in software-defined networking: A survey. *Comput. Netw.* **2015**, *92*, 189–207. [CrossRef]
14. Okoli, C.; Schabram, K. A guide to conducting a systematic literature review of information systems research. *Sprouts Work. Pap. Inf. Syst.* **2010**, *10*, 1–49. [CrossRef]
15. Nobre, J.; Rosario, D.; Both, C.; Cerqueira, E.; Gerla, M. Toward software-defined battlefield networking. *IEEE Commun. Mag.* **2016**, *54*, 152–157. [CrossRef]
16. Zacarias, I.; Gaspary, L.P.; Kohl, A.; Fernandes, R.Q.; Stocchero, J.M.; de Freitas, E.P. Combining Software-Defined and Delay-Tolerant Approaches in Last-Mile Tactical Edge Networking. *IEEE Commun. Mag.* **2017**, *55*, 22–29. [CrossRef]
17. Mihailescu, M.; Nguyen, H.; Webb, M.R. Enhancing wireless communications with software defined networking. In Proceedings of the 2015 IEEE Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 10–12 November 2015; pp. 1–6.
18. Phemius, K.; Seddar, J.; Bouet, M.; Khalifé, H.; Conan, V. Bringing SDN to the edge of tactical networks. In Proceedings of the 2016 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 1–3 November 2016; pp. 1047–1052.
19. White, K.; Denney, E.; Knudson, M.D.; Marnerides, A.; Pezaros, D. A programmable SDN+NFV-based architecture for UAV telemetry monitoring. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2016; pp. 522–527.
20. Kumar, R.; Hasan, M.; Padhy, S.; Evchenko, K.; Piramanayagam, L.; Mohan, S.; Bobba, R.B. Dependable End-to-End Delay Constraints for Real-Time Systems Using SDNs. *arXiv* **2017**, arXiv:1703.01641.
21. Spencer, J.; Willink, T. SDN in coalition tactical networks. In Proceedings of the 2016 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 1–3 November 2016; pp. 1053–1058.
22. Elgendi, I.; Munasinghe, K.S.; Mcgrath, B. A heterogeneous software defined networking architecture for the tactical edge. In Proceedings of the 2016 IEEE Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 8–10 November 2016; pp. 1–7.
23. Gupta, L.; Jain, R.; Vaszkun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1123–1152. [CrossRef]
24. Nguyen, H.X.; Webb, M.R.; Naguleswaran, S. Achieving policy defined networking for military operations. In Proceedings of the 2016 IEEE Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 8–10 November 2016; pp. 1–6.

25. Frøseth, I.M. Adding Network Services to Federated Networks. Master's Thesis, NTNU Trondheim, Trondheim, Norway, 2016.
26. Qing, J.; Yang, Y.; Jing, L.; Kun, M.; Huan, M.; Hao, D. An SDN-based resource pre-combination dispatching strategy in military network. In Proceedings of the Third International Conference on Cyberspace Technology (CCT 2015), Beijing, China, 17–18 October 2015.
27. Kroculick, J.B. Application of assurance-driven design to capability set management. In *2017 Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation*; International Society for Optics and Photonics: Bellingham, WA, USA, 2017; Volume 10205, p. 102050F.
28. Mishra, V.; Verma, D.; Williams, C.; Marcus, K. Comparing software defined architectures for coalition operations. In Proceedings of the 2017 IEEE International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 15–16 May 2017; pp. 1–7.
29. Armando, A.; Ranise, S.; Traverso, R.; Wrona, K. Compiling NATO authorization policies for enforcement in the cloud and SDNs. In Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 28–30 September 2015; pp. 741–742.
30. Wrona, K.; Oudkerk, S.; Szwaczyk, S.; Amanowicz, M. Content-based security and protected core networking with software-defined networks. *IEEE Commun. Mag.* **2016**, *54*, 138–144. [CrossRef]
31. Pham, T.; Cirincione, G.; Swami, A.; Pearson, G.; Williams, C. Distributed analytics and information science. In Proceedings of the 2015 IEEE 18th International Conference on Information Fusion (Fusion), Washington, DC, USA, 6–9 July 2015; pp. 245–252.
32. Mulec, G.; Vasiu, R.; Frigura-Iliasa, F. Distributed flow controller for mobile ad hoc networks. In Proceedings of the 2013 IEEE 8th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 23–25 May 2013; pp. 143–146.
33. Bouet, M.; Phemius, K.; Leguay, J. Distributed SDN for mission-critical networks. In Proceedings of the 2014 IEEE Military Communication Conference (MILCOM), Baltimore, MD, USA, 6–8 October 2014; pp. 942–948.
34. Soule, N.; Pal, P.; Clark, S.; Krisler, B.; Macera, A. Enabling defensive deception in distributed system environments. In *Resilience Week (RWS)*; IEEE: Chicago, IL, USA, 2016; pp. 73–76.
35. Dilmaghani, R.; Kwon, D. Evaluation of OpenFlow load balancing for navy. In Proceedings of the 2015 IEEE Military Communication Conference (MILCOM), Tampa, FL, USA, 26–28 October 2015; pp. 133–138.
36. Spencer, J.; Taylor, R.; Hancock, R. Evaluation of software-defined networking control plane performance in deployed military communications systems. In Proceedings of the 2017 IEEE International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 15–16 May 2017; pp. 1–7.
37. Athmiya, N.; Shobha, K.; Sarimela, V. Feasibility study and implementation of OpenFlow based SDN controller for tactical scenario. In Proceedings of the IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 20–21 May 2016; pp. 789–794.
38. Mishra, V.K.; Dasari, V.R. GENI Deployment and Research at US Army Research Laboratory. In Proceedings of the 2014 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 6–8 October 2014; pp. 995–1002.
39. Wrona, K.; Oudkerk, S. Integrated content-based information security for future military systems. In Proceedings of the 2015 IEEE Military Communications Conference (MILCOM), Tampa, FL, USA, 26–28 October 2015; pp. 1230–1235.
40. Mishra, V.; Verma, D.; Williams, C. Leveraging SDN for Cyber Situational Awareness in Coalition Tactical Networks. In Proceedings of the IST-148 Meeting, Sofia, Bulgaria, 3–4 October 2016.
41. Jalaian, B.; Dasari, V.; Hou, Y.T. Modeling and optimization for programmable unified control plane in heterogeneous wireless networks. In Proceedings of the 2016 IEEE 37th Sarnoff Symposium, Newark, NJ, USA, 19–21 September 2016; pp. 37–42.
42. McLaughlin, S.; Schutz, R.; Hancock, R.; Wrona, K.; Spencer, J.; Luoma, M.; Varis, N.; Mishra, V.K.; Carlén, P.; Belci, A.M. National mobility in coalition tactical networks. In Proceedings of the 2017 IEEE International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 15–16 May 2017; pp. 1–7.
43. Lee, K.; Kwon, B.; Kang, J.; Heo, S.; Lee, S. Optimal flow rate control for SDN-based naval systems. *IEEE Trans. Aerosp. Electron. Syst.* **2017**, *53*, 2690–2705. [CrossRef]

44. Wrona, K.; Amanowicz, M.; Szwaczyk, S.; Gierłowski, K. SDN testbed for validation of cross-layer data-centric security policies. In Proceedings of the 2017 IEEE International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 15–16 May 2017; pp. 1–6.
45. Nazari, S.; Du, P.; Gerla, M.; Hoffmann, C.; Kim, J.H.; Capone, A. Software Defined naval network for satellite communications (SDN-SAT). In Proceedings of the 2016 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 1–3 November 2016; pp. 360–366.
46. Spencer, J.; Worthington, O.; Hancock, R.; Hepworth, E. Towards a tactical software defined network. In Proceedings of the 2016 IEEE International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 23–24 May 2016; pp. 1–7.
47. Skappel, H.F. Traffic Policing in Dynamic Military Networks Using Software Defined Networking. Master's Thesis, NTNU Trondheim, Trondheim, Norway, 2016.
48. Lee, Y.; Kim, Y.; Lee, Y. Untraceable Blind Packet Forwarding Using Centralized Path Control. In Proceedings of the 2014 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 6–8 October 2014; pp. 268–273.
49. Li, G.; Xiang, Q.; Dearlove, C.; Yang, Y.R. A Self-Organizing SDN Architecture for Mobile Tactical Edge Networks. Available online: https://dais-ita.org/sites/default/files/S_028-paper.pdf (accessed on 9 September 2018).
50. Fagervoll, H.M. SDN in Heterogeneous Mobile Tactical Networks. Master's Thesis, NTNU Trondheim, Trondheim, Norway, 2017.
51. Chen, K.; Lv, N.; Zhao, S.; Wang, X.; Zhao, J. A Scheme for Improving the Communications Efficiency Between the Control Plane and Data Plane of the SDN-Enabled Airborne Tactical Network. *IEEE Access* **2018**, *6*, 37286–37301. [CrossRef]
52. Anderson, D. An investigation into the use of software defined networking controllers in aerial networks. In Proceedings of the 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 285–290.
53. Battiati, F.; Catania, G.; Ganga, L.; Morabito, G.; Mursia, A.; Viola, A. CSSS: Cyber security simulation service for software defined tactical networks. In Proceedings of the 2018 IEEE International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 531–533.
54. Zacarias, I.; Schwarzrock, J.; Gaspary, L.P.; Kohl, A.; Fernandes, R.Q.; Stocchero, J.M.; de Freitas, E.P. Employing SDN to control video streaming applications in military mobile networks. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–4.
55. Poularakis, K.; Iosifidis, G.; Tassiulas, L. SDN-Enabled Tactical Ad Hoc Networks: Extending Programmable Control to the Edge. *arXiv* **2018**, arXiv:1801.02909.
56. Du, P.; Pang, F.; Braun, T.; Gerla, M.; Hoffmann, C.; Kim, J.H. Traffic optimization in software defined naval network for satellite communications. In Proceedings of the 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 459–464.
57. Fongen, A.; Geir, K. Trust management in tactical coalition software defined networks. In Proceedings of the 2018 IEEE International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, 22–23 May 2018.
58. Iqbal, H.; Ma, J.; Stranc, K.; Palmer, K.; Benbenek, P. A software-defined networking architecture for aerial network optimization. In Proceedings of the 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, Korea, 6–10 June 2016; pp. 151–155.
59. Rendon, O.M.C.; Estrada-Solano, F.; Granville, L.Z. An approach to overcome the complexity of network management situations by mashments. In Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications (AINA), Victoria, BC, Canada, 13–16 May 2014; pp. 875–883.
60. Chadha, R.; Bowen, T.; Chiang, C.Y.J.; Gottlieb, Y.M.; Poylisher, A.; Sapello, A.; Serban, C.; Sugrim, S.; Walther, G.; Marvel, L.M.; et al. CyberVAN: A Cyber Security Virtual Assured Network Testbed. In Proceedings of the 2016 IEEE Military Communication Conference (MILCOM), Baltimore, MD, USA, 1–3 November 2016; pp. 1125–1130.
61. Ren, L.; Qin, Y.; Wang, B.; Zhang, P.; Luh, P.B.; Jin, R. Enabling resilient microgrid through programmable network. *IEEE Trans. Smart Grid* **2017**, *8*, 2826–2836. [CrossRef]

62. Chang, S.Y.; Park, Y.; Muralidharan, A. Fast address hopping at the switches: Securing access for packet forwarding in SDN. In Proceedings of the Network Operations and Management Symposium (NOMS), Istanbul, Turkey, 25–29 April 2016; pp. 454–460.
63. Kaleem, Z.; Li, Y.; Chang, K. Architecture and features for 5G mobile personal cell. In Proceedings of the 2015 IEEE International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 28–30 October 2015; pp. 164–166.
64. Pisharody, S.; Natarajan, J.; Chowdhary, A.; Alshalan, A.; Huang, D. Brew: A Security Policy Analysis Framework for Distributed SDN-Based Cloud Environments. *IEEE Trans. Depend. Secure Comput.* **2017**. [CrossRef]
65. Ashraf, U.; Yuen, C. Capacity-Aware Topology Resilience in Software-Defined Networks. *IEEE Syst. J.* **2017**, 1–10. [CrossRef]
66. Ionita, M.G.; Patriciu, V.V. Cyber Incident Response Aided by Neural Networks and Visual Analytics. In Proceedings of the 2015 20th IEEE International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 27–29 May 2015; pp. 229–233.
67. Tabata, S.; Ueda, K.; Fukui, R.; Shimazu, K.; Shigeno, H. Disaster information gathering system based on web caching and OpenFlow in unstable networks. In Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 17–24.
68. Skorin-Kapov, N.; Furdek, M.; Zsigmond, S.; Wosinska, L. Physical-layer security in evolving optical networks. *IEEE Commun. Mag.* **2016**, *54*, 110–117. [CrossRef]
69. Kaplan, M.; Zheng, C.; Monaco, M.; Keller, E.; Sicker, D. WASP: A software-defined communication layer for hybrid wireless networks. In Proceedings of the Tenth ACM/IEEE Symposium on Architectures for Networking and Communications Systems, Marina del Rey, CA, USA, 20–21 October 2014; pp. 5–16.
70. Liu, L.; Ye, Z.; Ito, A. CAMS: Coordinator assisted mobility support for seamless and bandwidth-efficient handover in ICN. In Proceedings of the 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, 6–10 December 2015; pp. 1–7.
71. Parker, T.; Johnson, J.; Tummala, M.; McEachen, J.; Scrofani, J. Dynamic state determination of a software-defined network via dual basis representation. In Proceedings of the 2014 IEEE 8th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, QLD, Australia, 15–17 December 2014; pp. 1–7.
72. Benton, K.; Camp, L.J.; Swany, M. Bongo: A BGP speaker built for defending against bad routes. In Proceedings of the 2016 IEEE Military communication conference (MILCOM), Baltimore, MD, USA, 1–3 November 2016; pp. 735–739.
73. Li, Y.; Hua, N.; Song, Y.; Li, S.; Zheng, X. Fast lightpath hopping enabled by time synchronization for optical network security. *IEEE Commun. Lett.* **2016**, *20*, 101–104. [CrossRef]
74. Yau, S.S.; Buduru, A.B.; Nagaraja, V. Protecting Critical Cloud Infrastructures with Predictive Capability. In Proceedings of the 2015 IEEE 8th International Conference on Cloud Computing (CLOUD), New York, NY, USA, 27 June–2 July 2015; pp. 1119–1124.
75. Sørensen, E. SDN Used for Policy Enforcement in a Federated Military Network. Master's Thesis, Institutt for telematikk, NTNU Trondheim, Trondheim, Norway, 2014.
76. Porras, P.A.; Cheung, S.; Fong, M.W.; Skinner, K.; Yegneswaran, V. Securing the Software Defined Network Control Layer. In Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 8–11 February 2015.
77. Dahan, D.; Mahlab, U. Security threats and protection procedures for optical networks. *IET Optoelectron.* **2017**, *11*, 186–200. [CrossRef]
78. Savas, S.S.; Habib, M.F.; Tornatore, M.; Dikbiyik, F.; Mukherjee, B. Network adaptability to disaster disruptions by exploiting degraded-service tolerance. *IEEE Commun. Mag.* **2014**, *52*, 58–65. [CrossRef]
79. Qadir, J.; Ali, A.; Yau, K.L.A.; Sathiaseelan, A.; Crowcroft, J. Exploiting the power of multiplicity: A holistic survey of network-layer multipath. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2176–2213. [CrossRef]
80. Macedo, D.F.; Guedes, D.; Vieira, L.F.; Vieira, M.A.; Nogueira, M. Programmable networks From software-defined radio to software-defined networking. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1102–1125. [CrossRef]

81. Machuca, C.M.; Secci, S.; Vizarreta, P.; Kuipers, F.; Gouglidis, A.; Hutchison, D.; Jouet, S.; Pezaros, D.; Elmokashfi, A.; Heegaard, P.; et al. Technology-related disasters: A survey towards disaster-resilient Software Defined Networks. In Proceedings of the 2016 IEEE 8th International Workshop on Resilient Networks Design and Modeling (RNDM), Halmstad, Sweden, 13–15 September 2016; pp. 35–42.
82. Schlesinger, C. Splendid isolation: Language-based security for software-defined networks. In Proceedings of the Workshop on Hot Topics in Software Defined Networking, Helsinki, Finland, 13 August 2012; pp. 79–84.
83. Ficco, M.; Avolio, G.; Battaglia, L.; Manetti, V. Hybrid simulation of distributed large-scale critical infrastructures. In Proceedings of the 2014 International Conference on Intelligent Networking and Collaborative Systems (INCoS), Salerno, Italy, 10–12 September 2014; pp. 616–621.
84. Hai, N.T.; Kim, D.S. Efficient load balancing for multi-controller in SDN-based mission-critical networks. In Proceedings of the 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), Poitiers, France, 19–21 July 2016; pp. 420–425.
85. Ahmed, M.E.; Kim, H.; Park, M. Mitigating dns query-based ddos attacks with machine learning on software-defined networking. In Proceedings of the 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 11–16.
86. Cox, J.H.; Chung, J.; Donovan, S.; Ivey, J.; Clark, R.J.; Riley, G.; Owen, H.L. Advancing Software-Defined Networks: A Survey. *IEEE Access* **2017**, *5*, 25487–25526. [CrossRef]
87. Rametta, C.; Schembra, G. Designing a Softwarized Network Deployed on a Fleet of Drones for Rural Zone Monitoring. *Future Internet* **2017**, *9*, 8. [CrossRef]
88. Li, T.; Zhou, H.; Luo, H.; Yu, S. SERvICE: A software defined framework for integrated space-terrestrial satellite communication. *IEEE Trans. Mob. Comput.* **2018**, *17*, 703–716. [CrossRef]
89. Wang, X.; Zhao, S.; Zhao, J.; Li, Y.; Zhao, H.; Jiang, Y. Service Customized Software-Defined Airborne Information Networks. In *International Conference on Space Information Network*; Springer: Singapore, 2016; pp. 256–265.
90. Rossi, T.; De Sanctis, M.; Cianca, E.; Fragale, C.; Ruggieri, M.; Fenech, H. Future space-based communications infrastructures based on high throughput satellites and software defined networking. In Proceedings of the 2015 IEEE International Symposium on Systems Engineering (ISSE), Rome, Italy, 28–30 September 2015; pp. 332–337.
91. Shi, L.; Lu, Z.; Qin, P.; Yao, H. OpenFlow based spatial information network architecture. In Proceedings of the 2015 IEEE International Conference on Wireless Communications & Signal Processing (WCSP), Nanjing, China, 15–17 October 2015; pp. 1–5.
92. Bertaux, L.; Medjiah, S.; Berthou, P.; Abdellatif, S.; Hakiri, A.; Gelard, P.; Planchou, F.; Bruyere, M. Software defined networking and virtualization for broadband satellite networks. *IEEE Commun. Mag.* **2015**, *53*, 54–60. [CrossRef]
93. Carey, M.F.; Chan, V.W. Internetworking service architecture for transporting mission-critical data over heterogeneous subnetworks with probabilistic guarantees. In Proceedings of the 2015 IEEE Military Communication Conference (MILCOM), Tampa, FL, USA, 26–28 October 2015; pp. 1002–1008.
94. Radhakrishnan, R.; Edmonson, W.W.; Afghah, F.; Rodriguez-Osorio, R.M.; Pinto, F.; Burleigh, S.C. Survey of Inter-Satellite Communication for Small Satellite Systems: Physical Layer to Network Layer View. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2442–2473. [CrossRef]
95. Brand, J.C. Protected transitional solution to transformational satellite communications. In *Digital Wireless Communications VII and Space Communication Technologies*; International Society for Optics and Photonics: Bellingham, WA, USA, 2005; Volume 5819, pp. 366–374.
96. Sturman, T.A.; Dingley, P.; Bowyer, M.D.; Petfield, N.R.; Moseley, M.; Fairhurst, G. Provisioning tactical MILSATCOM through DVB augmentation. In Proceedings of the 2008 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 16–19 November 2008; pp. 1–7.
97. Feng, J.; Jiang, L.; Shen, Y.; Ma, W.; Yin, M. A Scheme for Software Defined ORS Satellite Networking. In Proceedings of the 2014 IEEE Fourth International Conference on Big Data and Cloud Computing (BdCloud), Sydney, NSW, Australia, 3–5 December 2014; pp. 716–721.
98. Li, T.; Zhou, H.; Luo, H.; You, I.; Xu, Q. Multi-Strategy Flow Table Management for Software Defined Satellite Networks. *IEEE Access* **2017**, *5*, 14952–14965. [CrossRef]

99. Modieginyane, K.M.; Letswamotse, B.B.; Malekian, R.; Abu-Mahfouz, A.M. Software defined wireless sensor networks application opportunities for efficient network management: A survey. *Comput. Electr. Eng.* **2017**, *66*, 274–287. [CrossRef]
100. Aleksander, M.B.; Dubchak, L.; Chyzh, V.; Naglik, A.; Yavorski, A.; Yavorska, N.; Karpinski, M. Implementation technology software-defined networking in Wireless Sensor Networks. In Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Warsaw, Poland, 24–26 September 2015; Volume 1, pp. 448–452.
101. Li, W.; Liu, D.; Zhu, B.; Wei, X.; Xiao, W.; Yang, L. SDN control model for intelligent task execution in wireless sensor and actor networks. In Proceedings of the 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), Nanjing, China, 15–18 May 2016; pp. 1–5.
102. Zhou, J.; Jiang, H.; Wu, J.; Wu, L.; Zhu, C.; Li, W. SDN-based application framework for wireless sensor and actor networks. *IEEE Access* **2016**, *4*, 1583–1594. [CrossRef]
103. Kahjogh, B.O.; Bernstein, G. Energy and latency optimization in software defined wireless networks. In Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 4–7 July 2017; pp. 714–719.
104. Ndiaye, M.; Hancke, G.P.; Abu-Mahfouz, A.M. Software Defined Networking for Improved Wireless Sensor Network Management: A Survey. *Sensors* **2017**, *17*, 1031. [CrossRef] [PubMed]
105. Yuan, Z.; Huang, X.; Sun, L.; Jin, J. Software defined mobile sensor network for micro UAV swarm. In Proceedings of the 2016 IEEE International Conference on Control and Robotics Engineering (ICCRE), Singapore, 2–4 April 2016; pp. 1–4.
106. Zeng, D.; Miyazaki, T.; Guo, S.; Tsukahara, T.; Kitamichi, J.; Hayashi, T. Evolution of software-defined sensor networks. In Proceedings of the 2013 IEEE Ninth International Conference on Mobile Ad Hoc and Sensor Networks (MSN), Dalian, China, 11–13 December 2013; pp. 410–413.
107. Zeng, D.; Li, P.; Guo, S.; Miyazaki, T.; Hu, J.; Xiang, Y. Energy minimization in multi-task software-defined sensor networks. *IEEE Trans. Comput.* **2015**, *64*, 3128–3139. [CrossRef]
108. Sayyed, R.; Kundu, S.; Warty, C.; Nema, S. Resource optimization using software defined networking for smart grid wireless sensor network. In Proceedings of the 2014 3rd International Conference on Eco-friendly Computing and Communication Systems (ICECCS), Mangalore, India, 18–21 December 2014; pp. 200–205.
109. Letswamotse, B.; Modieginyane, K.; Malekian, R. SDN Based QoS Provision in WSN Technologies. *arXiv* **2017**, arXiv:abs/1702.08164.
110. Abels, T.; Khanna, R.; Midkiff, K. Future proof IoT: Composable semantics, security, QoS and reliability. In Proceedings of the 2017 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet), Phoenix, AZ, USA, 15–18 January 2017; pp. 1–4.
111. Fortino, G.; Di Fatta, G.; Pathan, M.; Vasilakos, A.V. Cloud-assisted body area networks: State-of-the-art and future challenges. *Wirel. Netw.* **2014**, *20*, 1925–1938. [CrossRef]
112. Junli, F.; Yawen, W.; Haibin, S. An improved energy-efficient routing algorithm in software define wireless sensor network. In Proceedings of the 2017 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xiamen, China, 22–25 October 2017; pp. 1–5.
113. Gonzalez, C.; Charfadine, S.M.; Flauzac, O.; Nolot, F. SDN-based security framework for the IoT in distributed grid. In Proceedings of the 2016 IEEE International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, Croatia, 13–15 July 2016; pp. 1–5.
114. Ionita, M.G.; Patriciu, V.V. Secure Threat Information Exchange across the Internet of Things for Cyber Defense in a Fog Computing Environment. *Inf. Econ.* **2016**, *20*, 16. [CrossRef]
115. Singh, D.; Tripathi, G.; Alberti, A.M.; Jara, A. Semantic edge computing and IoT architecture for military health services in battlefield. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 185–190.
116. Tortonesi, M.; Michaelis, J.; Morelli, A.; Suri, N.; Baker, M.A. SPF: An SDN-based middleware solution to mitigate the IoT information explosion. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–30 June 2016; pp. 435–442.
117. Moy, C.; Palicot, J. Software radio: A catalyst for wireless innovation. *IEEE Commun. Mag.* **2015**, *53*, 24–30. [CrossRef]
118. Ulversoy, T. Software defined radio: Challenges and opportunities. *IEEE Commun. Surv. Tutor.* **2010**, *12*, 531–550. [CrossRef]

119. Kacpura, T.J.; Eddy, W.M.; Smith, C.R.; Liebetreu, J. Software defined radio architecture contributions to next generation space communications. In Proceedings of the 2015 IEEE Aerospace Conference, Big Sky, MT, USA, 7–14 March 2015; pp. 1–12.
120. Sigholm, J.; Raciti, M. Best-effort Data Leakage Prevention in inter-organizational tactical MANETs. In Proceedings of the 2012 IEEE Military communication conference (MILCOM), Orlando, FL, USA, 29 October–1 November 2012; pp. 1–7.
121. Cormier, A.R.; Dietrich, C.B.; Price, J.; Reed, J.H. Dynamic reconfiguration of software defined radios using standard architectures. *Phys. Commun.* **2010**, *3*, 73–80. [CrossRef]
122. Androlewicz, J.F.; Buffington, R.L.; Kief, C.J.; Erwin, R.S.; Crane, J.; Avery, K.; Lyke, J. Software-defined and cognitive radio technology for military space applications. In Proceedings of the Wireless Innovation Forum Conference on Communications Technologies and Software Defined Radio, Washington, DC, USA, 4 October 2011.
123. Moessner, K.; Bourse, D.; Greifendorf, D.; Stammen, J. Software radio and reconfiguration management. *Comput. Commun.* **2003**, *26*, 26–35. [CrossRef]
124. Noble, J.; Liem, D.T.; Tuan, N.Q.; Luat, D.; Asharif, M.R. Battalion-organic electronic fires: A tactical application of commercial unmanned systems and software-defined radios. In Proceedings of the 2017 IEEE Third Asian Conference on Defence Technology (ACDT), Phuket, Thailand, 18–20 January 2017; pp. 20–25.
125. North, R. Joint Tactical Radio System-connecting the GIG to the tactical edge. In Proceedings of the 2006 IEEE Military Communications Conference (MILCOM), Washington, DC, USA, 23–25 October 2006; pp. 1–6.
126. Wei, J.; Ji, Y.; Yu, C. Improvement of Software Defined Radio based RSSI localization with bias reduction. *IFAC Proc. Vol.* **2014**, *47*, 7164–7169. [CrossRef]
127. Wang, H.; Crilly, B.; Zhao, W.; Autry, C.; Swank, S. Implementing mobile ad hoc networking (MANET) over legacy tactical radio links. In Proceedings of the 2007 IEEE Military Communications Conference (MILCOM), Orlando, FL, USA, 29–31 October 2007; pp. 1–7.
128. Almoualem, F.; Satam, P.; Ki, J.G.; Hariri, S. SDR-Based Resilient Wireless Communications. In Proceedings of the 2017 International Conference on Cloud and Autonomic Computing (ICCAC), Tucson, AZ, USA, 18–22 September 2017; pp. 114–119.
129. Casini, E.; Street, M.; Vigneron, P.; Barfoot, R. *SDR-Ready Standardized Waveforms for Tactical VHF and UHF Communications for NATO*; Technical Report; NATO C3 Agency: Hague, The Netherlands, 2010.
130. Singh, S.; Adrat, M.; Antweiler, M.; Ulversoy, T.; Mjelde, T.; Hanssen, L.; Ozer, H.; Zumbul, Z. Acquiring and Sharing Knowledge for Developing SCA Based Waveforms on SDRs. Available online: https://pdfs.semanticscholar.org/f490/1fe9efd522d3411bd935d18095c9d369320d.pdf (accessed on 9 September 2018).
131. Jover, R.P.; Lackey, J.; Raghavan, A. Enhancing the security of LTE networks against jamming attacks. *EURASIP J. Inf. Secur.* **2014**, *2014*, 7. [CrossRef]
132. Kaur, H.; Kaur, A.; Khanna, D. Benchmarking of AODV Routing Protocol Implemented for Military Software Defined Radio Waveform. *Int. J. Comput. Appl. Found. Comput. Sci.* **2015**, *120*, 39–42. [CrossRef]
133. Mahasamudram, A.R.; Srinivasaiah, R.; Raveendranath, K.; Ramanath, S. Agile cognizant transceiver link for mission critical applications. In Proceedings of the 2016 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 1–3 November 2016; pp. 1137–1142.
134. Kwak, K.J.; Sagduyu, Y.; Yackoski, J.; Azimi-Sadjadi, B.; Namazi, A.; Deng, J.; Li, J. Airborne network evaluation: Challenges and high fidelity emulation solution. *IEEE Commun. Mag.* **2014**, *52*, 30–36. [CrossRef]
135. Moura, D.F.C.; da Silva, F.A.B.; Galdino, J.F. Case Studies of Attacks over Adaptive Modulation Based Tactical Software Defined Radios. *J. Comput. Netw. Commun.* **2012**, *2012*. [CrossRef]
136. Amjad, M.; Akhtar, F.; Rehmani, M.H.; Reisslein, M.; Umer, T. Full-Duplex Communication in Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2017**. [CrossRef]
137. Chandrasekharan, S.; Gomez, K.; Al-Hourani, A.; Kandeepan, S.; Rasheed, T.; Goratti, L.; Reynaud, L.; Grace, D.; Bucaille, I.; Wirth, T.; et al. Designing and implementing future aerial communication networks. *IEEE Commun. Mag.* **2016**, *54*, 26–34. [CrossRef]
138. Cao, Z.; Johansson, P.; Hodgkiss, W.; Zhao, W.; Nwokafor, A.; Cuenco, J.; Hobson, B. Design and rapid prototyping of SCA-compliant public safety P25 waveform and P25–FM3TR–VoIP bridge. *Analog Integr. Circuits Signal Process.* **2011**, *69*, 245. [CrossRef]
139. Favraud, R.; Apostolaras, A.; Nikaein, N.; Korakis, T. Toward moving public safety networks. *IEEE Commun. Mag.* **2016**, *54*, 14–20. [CrossRef]

140. Lal, C.; Petroccia, R.; Conti, M.; Alves, J. Secure underwater acoustic networks: Current and future research directions. In Proceedings of the 2016 IEEE Third Underwater Communications and Networking Conference (UComms), Lerici, Italy, 30 August–1 September 2016; pp. 1–5.
141. Baldini, G.; Picchi, O.; Luise, M.; Sturman, T.A.; Vergari, F.; Moy, C.; Braysy, T.; Dopico, R. The EULER project: Application of software defined radio in joint security operations. *IEEE Commun. Mag.* **2011**, *49*, 55–62. [CrossRef]
142. Adrat, M.; Osten, T.; Leduc, J.; Antweiler, M.; Elders-Boll, H. On considering hierarchical modulation in the porting process of legacy waveforms to software defined radio. *Analog Integr. Circuits Signal Process.* **2014**, *78*, 729–739. [CrossRef]
143. Bader, A.; Alouini, M.S. Mobile Ad Hoc Networks in Bandwidth-Demanding Mission-Critical Applications: Practical Implementation Insights. *IEEE Access* **2017**, *5*, 891–910. [CrossRef]
144. Bor-Yaliniz, I.; Yanikomeroglu, H. The new frontier in RAN heterogeneity: Multi-tier drone-cells. *IEEE Commun. Mag.* **2016**, *54*, 48–55. [CrossRef]
145. Mahmoud, S.; Jawhar, I.; Mohamed, N.; Wu, J. UAV and WSN softwarization and collaboration using cloud computing. In *Smart Cloud Networks & Systems (SCNS)*; IEEE: Dubai, United Arab Emirates, 2016; pp. 1–8.
146. Akyildiz, I.F.; Wang, P.; Lin, S.C. SoftWater: Software-defined networking for next-generation underwater communication systems. *Ad Hoc Netw.* **2016**, *46*, 1–11. [CrossRef]
147. Fan, R.; Mc Goldricky, C.; Gerla, M. An SDN architecture for under water search and surveillance. In Proceedings of the 2017 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Jackson, WY, USA, 21–24 February 2017; pp. 96–99.
148. Demirors, E.; Shankar, B.G.; Santagati, G.E.; Melodia, T. SEANet: A software-defined acoustic networking framework for reconfigurable underwater networking. In Proceedings of the 10th International Conference on Underwater Networks & Systems, Arlington, VA, USA, 22–24 October 2015; p. 11.