Review

Software-Defined Networking for Unmanned Aerial Vehicular Networking and Security: A Survey

James McCoy and Danda B. Rawat *

Data Science and Cybersecurity Center (DSCC), Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059, USA; james.mccoy@bison.howard.edu

* Correspondence: db.rawat@ieee.org; Tel.: +1-202-806-2209

Received: 20 September 2019; Accepted: 22 November 2019; Published: 3 December 2019

Abstract: Despite the immense benefits offered by the utilization of unmanned aerial vehicles (UAVs) in civilian and military applications, significant work needs to be done to ensure that these systems are able to securely communicate and resiliently operate to accomplish the mission. As the UAVs grow with their popularity and usability for different applications, there is a dire need to ensure that UAVs and their networks are capable of mitigating cyber-attacks on the fly. One approach that has gained considerable popularity is Software-Defined Networking (SDN) based solutions. SDN is a networking paradigm that has gained attention due to its dynamic flexibility to program networks and increase network visibility, and its potential to assist in the mitigating security vulnerabilities in the network including the network of UAVs. This article provides an overview of recent advances, and current state of art related to security vulnerabilities and SDN enabled countermeasures. This paper also presents a comparison of different approaches in a tabular form and a discussion of challenges and future research directions with respect to UAV security.

Keywords: software-defined networking (SDN); unmanned aerial vehicle (UAV) security

1. Introduction

In recent years, Unmanned Aerial Vehicles (UAVs) have gained considerable popularity with military, civilian, and public organizations for their diverse applications [1–4]. UAVs are currently deployed for numerous mission types including investigations, border surveillance, delivery services, traffic monitoring, and environmental monitoring. Most importantly, the military has used this technology with the broad goal of leveraging its immense potential to improve national security for sensitive combat missions. By 2035, the Department of Defense (DoD) expects that the percentage of unmanned vehicles will grow from 25% of their military fleet to approximately 70% [5]. The U.S. military increased its investment in research and development of UAV technology from \$2.3 billion in 2008 to \$4.2 billion in 2013 [6]. Moreover, Rani et al. [7] highlighted that the Federal Aviation Administration estimated that by 2020, U.S. will have more than 30,000 drones actively operating in the US airspace. The continued growth and innovation of UAV related technology has increased device accessibility while concurrently making the device a more cost effective and powerful platform [7].

The continued growth and innovation of UAV related technology will allow for more accessible, cheaper, and more effective unmanned systems [8]. Given the broad use of this technology one emerging concern is security and reliability of the UAV communication networks. Many advancements have been made in this technology but numerous challenges have to be addressed related to the ability for the devices to communicate securely. Secure communication is increasingly becoming more important because these devices are performing a central role in civilian and military operations. Network vulnerabilities can result in unauthorized access to sensitive or critical mission information ultimately posing a threat to National security. For example, in 2009, Iranian-backed Shiite militants

hacked the live feed of a Predator drone using an online software called SkuGrabber, which allowed insurgents access to the drone's encrypted data [9,10]. Software-Defined Networks (SDNs) are increasingly being explored to mitigate many network vulnerabilities. SDN is a networking technology that provides programmability and network visibility for management and security [11] by separating hardware, control, and data planes of the networking infrastructure. The separation of a network's control structure and communication infrastructure is replaced by a programmable control layer. This layer allows the configuration of the network's essential functionality [11,12]. The implementation of SDN into UAV networking differs greatly from rest of the networks because of the network vector and attack surfaces which are being attacked.

The purpose of this study is to provide a comprehensive review of SDN based security solutions that have been adopted to mitigate UAV network attacks. Specifically, this paper focuses on mitigation techniques that are based on SDN system and its capability to combat cyber attacks on UAV systems. Note that there are several solutions based on SDN for general networks which are not included if those approaches are not relevant to UAV networks. Although there are some related papers on UAV security (for further details, please refer to Section 4), we present peer-reviewed security solutions on the rapidly advancing research field of SDN enabled UAV networks. Specifically, the main contributions of this paper include:

- Presenting a comprehensive study on security aspects of SDN enabled UAV networks.
- Presenting a summary of attacks and countermeasures for SDN enabled UAV networks in a tabular form for a side-by-side comparison.
- Presenting a discussion of research challenges, recent trends, insights and open problems for SDN enabled UAV security.

The rest of the paper is organized as follows: Section 2 provides a brief historical overview of notable advances in UAV technology, Section 3 provides UAV network architecture and communication. Section 4 discusses the SDN architecture and its security features. Section 5 presents SDN implementation in UAV networks and followed by SDN enabled UAV network security in Section 7. Section 8 discusses open research issues. Section 9 concludes the paper.

2. Brief Timeline of Advances in UAVs

Early interest in UAV systems was sparked as militaries were looking to develop battlefield technologies. UAVs were first operationalized by the United States during the Vietnam War. The Air Force program entitled Lightning Bug used early UAVs during tactical reconnaissance missions and was dispatched nearly 3500 times during that period [5]. The success of this program is predicated upon the ability for continued operations in war zones without risking the lives of pilots [13]. The expanded use of UAVs allowed for missions to occur that were outside of human limitations (Gertler 2012). Ongoing military operations in the Middle East sparked a renewed interest in UAVs with Israel serving as one of the first nations to deploy these devices regularly, demonstrating their effectiveness in combat operations [14].

Civilian interest in UAVs led to innovation in build material and increase flight durability in UAV technologies [15]. Also, the development of fully autonomous flight technology allowed the military to deploy military drones in military operations requiring lethal force [16]. The 11 September 2001 attack on the World Trade Center further pushed the drone technology as military operators sought to leverage drone technology for counterterrorism operations. Following the attacks of September 11th, UAVs have continued to maintain a central role function in military operations. The continued push to implement technologies that are able to adapt to the current battlefield needs has led to a class of UAVs that maintain advanced capabilities but are increasingly becoming commercialized due to the availability of the technology. Figure 1 presents a timeline of significant events in the growing use of UAV technology.

Figure 1. Historical Timeline of Unmanned Aerial Vehicles (UAVs).

3. UAV Network Architecture and Communications

Section 3 dissects network architecture and communications and is sectioned in the following manner. Section 3.1 details the UAV network architecture. Section 3.2 presents flying ad-hoc networking and routing. The conclusion, in Section 3.3, explores communications in UAV networks and vulnerability.

3.1. UAV Network Architecture

A typical UAV network architecture is shown in Figure 2. Data communication in UAVs along with associated networks is highly important in that it ensures the active UAV devices operate as intended to accomplish mission goals. The types of communication among UAV devices can be either categorized as UAV to UAV (U2U) communication or UAV to Infrastructure (U2I) communications, as shown in Figure 2. UAVs communication using U2U or U2I communications is critical since it facilitates to meet the mission to be achieved by using UAVs for a wide array of applications such as military, environmental, agricultural, commercial, and civilian applications. As UAV devices operate in open wireless environments, UAV network suffers from interferences from others as well as security attacks from adversaries.

Figure 2. A typical UAV networks with communication links with ground control station, aka Ground Data Acquisition Unit (GAU) and satellite.

One necessary aspect of effective UAV communication is the ability of these devices to securely communicate in an effective manner to meet the goal of the assigned mission. Collaborative communication is regarded as an ability for UAVs to communicate with other UAV devices as well as to the ground control stations, as shown in Figure 2. Moreover, effective UAVs should be capable of acting as communication relay nodes which can connect flying ad hoc networks (FANET) clusters. Within this network, the ability for UAV devices to serve as relay ensures communication is always available using either single hop or multi-hop communications. UAVs acting as network gateways provide connectivity to the infrastructure such as satellite or ground stations, or backbone networks in the occurrence they are being used in distant geographic areas or areas distracted by natural or man-made calamities. Other important requirements that facilitate seamless communication in the UAV architecture are data processing, data storage, assisted sensing, and centralized control.

Since UAVs are pilot-less (no direct human operators on-board) and depend on the communication and guidance of ground control stations or satellite station, it is necessary that communication networks remain highly secure from potential network attack for resilient UAV operations. Communication between UAVs and ground control stations are accomplished through a temporarily created UAV gateway of the UAV network formed on the fly. However, the UAV network has several security challenges given the frequently changing network topologies, network connectivity, and the high mobility of UAVs.

UAV network security can be increasingly challenging as these devices operate in a dynamic environment with significant resource constraints. Given this, security solutions for UAVs may derive from resource issues such as limited communication bandwidth, computational capabilities, and energy making wired networks such as Kerberos and transport layer security (TLS) impractical. Mahmoud et al. [17], proposed a network architecture that can facilitate a secure communication between UAVs and ground stations. The architecture is capable of supporting the specifications and requirements of UAV networks where the architecture supports cryptographic primitives to secure communication between airborne UAVs and ground stations.

3.2. Flying Ad-Hoc Network and Routing

UAVs equipped with computing, communication, storage and control devices form a flying ad hoc network (FANET) to communicate with each another and with the infrastructure. The networking layer is responsible for handling end-to-end routing of data packets being communicated through the network. However, FANETs lack a central control and fixed topology, thus causing challenges during the routing processes. As such, the choice of a suitable networking protocol for UAV to UAV communication is dependent upon several factors [18]; the total number of UAVs in FANET; different protocols provide excellent performance in small networks supporting few UAVs but may not provide such performance in a large UAV network; the limited processing capabilities implemented on-board; the routing protocol with limited processing and storage capabilities that can handle complex calculations; storage capacity and on-board memory; some routing protocols need a big storage space especially where mobile nodes are in large quantities; limited power and energy capabilities in UAVs; routing protocols that are energy-aware are more suitable for small sized UAVs compared to large UAVs; and heavily dependent on GPS capability (specially for geographic routing protocols). Other important factors to consider are security and transmission robustness, roaming and hand-off, connectivity to the backbone infrastructure network, degree at which UAVs are mobile, and overall throughput of the FANET. Furthermore, Oubbati et al. [19], have pointed out that it is a daunting task to design and develop an effective routing solution that ensures transferred data is delivered to the intended recipients in a UAV environment. The challenges caused by the difficulties of obtaining shortest connected and end-to-end pattern due to the high mobility of UAVs. Therefore, Oubbati et al. [19], proposed routing protocol for overcoming the above-mentioned challenges once implemented in FANETs of highly mobile UAVs.

FANET is expected to have seamless communication using communications among UAVs and ground stations which helps UAVs make informed decision while cooperating for a given mission [20,21]. For instance, in scenarios that require an adaptive application due to the varying nature of the missions, a real-time communication is needed to disseminate information and tasks within the network. Therefore, a persistent network connection is needed to facilitate the dissemination of information.

3.3. Communications in UAV Networks and Vulnerabilities

UAV communications suffer due to limited bandwidth. The work in [22] conducted a research aiming to resolve the bandwidth disruptions associated with pre-measurement in a network thus negatively impacting the performance in UAV networks for collecting crucial information such as condition of war zone, weather patterns, etc. [22]. UAVs are expected to collect data and process that data locally at UAVs or transfer that data to base stations to get the processed information back to UAV. Transferring massive amounts of data consequently utilizing most of the bandwidth in the network. This vulnerability invites security attacks (while data in motion) and other risks such as network failure due to bottleneck because of limited bandwidth for data transfer. UAVs may also fail to establish communication links with ground control stations leading to dangerous consequences for the UAVs and the mission handled by those UAVs. The network latencies caused by UAVs or data transfer may negatively impact the network's security exposing the network to attacks such as buffer overflow attacks, jamming attacks and distributed denial of service attacks (e.g., [22]). Furthermore, most UAVs are dependent on remotely located humans for control and coordination. When the bandwidth is inadequate, UAVs are likely to crash.

4. Software Defined Networking (SDN) Architecture and Its Features

This section provides software defined networking (SDN) architecture and its features for UAV system. Section 4.1 describes a typical SDN architecture. Section 4.2 follows with SDN features for network security.

4.1. A Typical SDN Architecture

The ideas that innovated into SDN have been around for over twenty years [11,23], but the applications of SDN and improvements related to SDN are emerging every day. For example, the General Switch Management Protocol (GSMP) released in 1996 by Ipsilon, the Tempest in 1998 by Cambridge, Forwarding and Control Element Separation (FORCES) protocol in 2000 by IETF and Path Computation Element (PCE) in 2004 by IETF are some of the most critical milestones of SDN development. PCE is a focused component for registering the way for the system hubs. Alongside Openflow, it is one of the principle approaches towards SDN. Additionally, essential aspects include the Routing Control Platform in 2004 by Princeton and a 4D (choice, dispersal, discovery, and information) way to deal with division of control rationale from systems administration components, in 2005. For some specialists, SDN began advancing when the ideas of SDN were first investigated in the Ethane venture at Stanford University in 2007 [11,23]. Standardization of Openflow as the principal correspondence interface for SDN by the Open Network Foundation in 2009 was the distinct advantage. Since then there have been several advancements in SDN architecture and efficiency, and SDN based security [11]. The overall promise of SDN is based upon the forwarding hardware decoupled from the network control components [11], as shown in Figure 3. Specifically, SDN architecture consists of three layers: application layer, controller layer, and infrastructure layer. Furthermore, the SDN controller layer controls the overall network functions. This layered configuration simplifies the networking paradigm and provides opportunities to improve network management practices. What is most intriguing about this emerging networking paradigm that separates the networks control structure from the underlying infrastructure layer [11,24]. The separation of the network's control structure and communication infrastructure has been replaced by a programmable control layer, allowing for the

configuration of the network's behavior. In traditional networking systems, the network is responsible for both the control and communication functions, which poses unique challenges as the infrastructure and the packet control functions were interrelated.

Figure 3. A typical software defined networking architecture.

The network infrastructure layer of the SDN model is similar to more traditional networking systems as it includes networking devices that are directly responsible for handling packet data as opposed to having to deal with networking traffic as well as complicated software-centered decisions [25]. The control layer is the intermediate layer between the network infrastructure layer and the application layer [26] which controls networking functions via programmable APIs. The emergence of programmable control interface such as OpenFlow has offered a variety of ways to handle network functions. For the most part, innovations in the control layer allow users to directly control network functionality. One benefit of having a programmable networking interface is that network control becomes centralized and is optimized by operators to meet the direct needs of the application [11]. The application layer houses the business logic that determines how resources are utilized [11]. Applications which run on the SDN network structure are responsible for communicating and controlling behaviors for programmatically controlling the network behaviors of the control layer. SDN has been used for different applications encompassing energy efficiency, security, network visibility through its ability to define a protocol stack [11,27–29]. Recently, there have been research works for incorporating SDN for UAV networks to make the UAV network more flexible and assist in effective functionality. By implementing SDNs in UAV networks, it is easier to deploy the UAV network which facilitates the control and management of network services and applications.

4.2. SDN Features for Network Security

SDN has several features that are highly beneficial to network security including dynamic control flow, centralized control providing visibility of the entire network, a simplified data plane, and network programmability.

Dynamic Flow Control: The data plane of SDN has a flow rule for handling the traffic flows in the network. As a result, a network application is capable of dynamically controlling the network flows [29]. The ability to control network flows is beneficial to network security due to several reasons. First and foremost, it makes it possible to implement control functions for providing dynamic access thus protecting the network from third-party access [30]. SDN networks, unlike traditional networks, have network devices such as OpenFlow switch capable of supporting SDN functions used in access control. Moreover, SDNs facilitate in the control of network flows which allows for increased granularity, enabling more efficient control of network flows. Furthermore, dynamic control benefits network security as it permits the separation of suspicious network flows from benign network flows [31]. For example, implementing an intrusion detection system in a traditional network will lead to the detection of malicious flows but will require the use of other methods such as honeypot systems to investigate the flows. Applying SDN as a network security measure eliminates the need for third-party systems since through dynamically controlling the network function, it is possible to build such a feature.

Increased visibility due to centralized control: The linking via the control plane allows disperse networks to receive control instructions. The control plane sends query messages to all data planes collecting the network information and status from all data planes [29]. Increased visibility improves network security by providing round-the-clock monitoring [32]. In traditional networks, effective monitoring would require the implementation of monitoring sensors in all network devices or links, which might be a challenge in large networks. The leveraging of a holistic view of the network facilitates the defense and detection of attempted network attacks. Greater insight allows security practitioners to adopt an anomaly analysis enabling them to pinpoint attacks on any part of the network. Also, the network-wide view leads to an improvement in utilizing security products and devices by assigning particular network flows to the needed security appliances [33]. The holistic view of the entire network provided for by the implementation of SDN leads to an understanding of the particular routes network flows pass through facilitating the installation of various security appliances.

Simplified data plane: As previously noted, within an SDN architecture, the data plane is separated from the control plane. As a result, the data plane can be controlled via user-defined logic. The simplification of the data plane makes it possible to equip it with new features. For example, in contrast with traditional network devices, the hardware of the network, that is the data plane, of SDN networks can be modified with ease [34]. This is because the SDN's data plane is separated from the complex control plane, and as such, its hardware modules are relatively simple. This feature makes it possible to modify the data plane and equip it with new network security features and functions. The SDN data plane can also be extended to modify and suit specific security purposes. Compared to other networking architectures, the data plane of SDN network can be modified to meet the security needs of a network in the case a new form of threat or attack has been detected [35]. Other networks whose data planes are connected to the control plane contain a lot of complicated modules rendering modifications impossible. The detection of new types of threats may warrant the complete overhaul of the networks to equip them with data planes capable of handling such threats. The simplicity of the data plane allows the addition of new security components which lead to the data plane being more scalable and containing the latest security functionalities.

Network Programmability: The SDN has a programmable network such that it is possible to program the network to operate various security functions [11,36]. This is a highly valued security feature because, in traditional network systems, hardware middleboxes are deployed with predefined network security functions. However, it is nearly impossible to modify the functions to suit a specific security need. In some scenarios, the predefined security functions may not be adequate in mitigating

an identified security risk or an attack. However, the programmability feature offered by SDN eliminates such problems by allowing the programming of various security functions with ease. For instance, it is possible to create an application for scanning and detecting security vulnerabilities in a network or to implement intelligent security applications in the network for detecting specific attacks such as DoS/DDoS attacks [29]. Network programmability not only leads to improved network security, but it is also cost effective in that it does not require the acquisition and deployment of new security products, which is a huge benefit compared to security in traditional network architectures.

Implementing SDN for UAVs is beneficial since SDN provides programmable and elastic network infrastructure which facilitate effective management of dissimilar protocols and overall network visibility [37]. SDN has features which makes it the best network to be used in unmanned aerial vehicles.

5. SDN Based UAV Network

Section 4 explores SDN based UAV network security vulnerabilities and the degree that SDN based networks can be leveraged to minimize these

A typical SDN enabled UAV network is depicted in Figure 4. In SDN, the communication or the interaction between the control layer and data link layer is commonly done using the OpenFlow protocol. Openflow is a distinct communication protocol that allows the network's forwarding plane control over the networks switch or router functionality. Its broader flexibility and control of the network and core functionality makes SDN attractive for overcoming many of the challenges with managing an airborne network. The first challenge is that UAV devices relay considerable information to either other UAV devices or the ground station such as the flight and control information of the UAV, information of the protocol stack in the UAV network, sensory information of UAVs and information obtained from the ground terminals. The next challenge with respect to managing UAV networks is that UAVs operate as moving objects. Unpredictable movement patterns have direct implications on the network's topology and wireless connections. The expected fluidity of the network produces another challenge that SDN seeks to overcome.

Figure 4. Typical components of a Software Defined Networking (SDN) based UAV network.

Several studies have highlighted the various ways that SDN can make UAV network more secure. Packet delivery ratio by tuning network speeds in an SDN-based UAV network exceeds other traditional ad hoc routing protocol [38]. Furthermore, SDN can adjust the UAV network topology in prediction of future changes by using knowledge of physical relationships through SDN controller [38]. In the SDN based UAV network, UAVs implement SDN features and the ground station such as the SDN controller as well as user equipment (UE) for control failures.

In the SDN-based UAV network, parameters of UAVs and network statistics are collected by the SDN controller. After that, the final optimal decision is taken by utilizing the precise computed results. The functional architecture of the UAV network is shown in Figure 5 with SDN controllers for the UAV network. The UAV controller manages information such as physical location, battery storage, and flight control and the SDN controller is to interact with the UAV controller and distribute the information about UAVs network. When the SDN controller detects a poor wireless link state, a message is sent to the UAV controller by the SDN controller. Then, the UAV adjusts the position with the intention of having an improved and stable communication link according to the command of the UAV controller. Significant strategies can be made based on the analysis and management of these statistics, which are from the network and UAVs. As mentioned earlier, managing the vast bulk of data is a problem.

Figure 5. Block diagram of UAV network architecture.

Moreover, the limited energy resources put constraints on communication duration and performance. Therefore, the full utilization of energy sources is required. To solve this problem, Mozaffari et al. [38] implemented a monitoring platform, as shown in Figure 6. The platform consists of four modules: monitoring display, flow management, strategies, and link management. The monitoring display module acts as the GUI to the user and provides system status to the user. The flow management module controls network flow by creating a set of configuration parameters to dictate how network traffic flows.

Figure 6. Architecture of Monitoring Platform for a UAV System.

Within this SDN architecture, packets are transmitted from one network endpoint to another. These endpoints may be a TCP/UDP port and IP address, etc. Dynamical management of the link load is done by the link management module by receiving updates from the UAV and other modules into considerations. The strategy module is responsible for developing algorithms and protocols. This development depends on the demand of the application. There are some other modules in this architecture and they are responsible for collecting information and performing calculations. The work of Mozaffari [38] focuses on the degree that SDN can solve many of the issues that were discussed above as it pertains to traditional networks.

6. Cyber Attacks in UAV Networks and SDN-Based Countermeasures

Section 5 presents cyber attacks in UAV networks with a focus on SDN-based countermeasures.

The security in a UAV network is crucial and before implementing any security mechanisms, it is essential to assess and analyze the network thoroughly. A full network assessment discovers existing vulnerabilities guiding the most appropriate security mechanisms that could be implemented. Lee et al. [39], posit that developing a full and systematic understanding of all attack surfaces in emergent networks is a necessity and proposed implementing measures for making the network more secure. Lee et al. [39] also argue that previous studies have been mostly dependent on ad-hoc practical techniques when the different elements of SDN networks are evaluated using different perspectives. These methods nevertheless fail to provide a systematic methodology nor do they provide automated systems that can be used to conduct rigorous security assessments in SDN networks and identify security flaws. However, with the recent research advancements in the SDN, it has emerged a promising technology to provide solutions for security concerns. Table 1 presents the SDN mitigation solutions discussed below.

A basic architecture of SDN networks has a control plane which detects the malfunctioning of targeted networking or sensing devices of UAV networks. Subsequently, the SDN's control plane mitigates impacts caused by sensor or actuator attacks by sending a set of instructions to the nodes of the affected UAV network from the SDN controller. The SDN controller identifies the nodes that have been injected with false or corrupt data and instruct the unaffected nodes to stop communication or route any messages from the affected nodes. This mechanism reduces vulnerability and possible impacts of the attacks on UAV networks.

Table 1. SDN Based Security Countermeasures.

Attack Type	SDN-Based Attack Mitigation	Pros and Cons
DDoS	Packet Flow Analysis [40]	Pros: + Efficient Detection of denial of services attacks + Achieves Optimal Network effectiveness Cons: - Imposes an overhead to network usage performance - Also imposes overhead to network access
DDoS	Machine Learning algorithms [41]	Pros: + Light weight detection protocol based on entropy variation analysis + Efficient detection rate over packet flow rate Cons: - Can only detect single host target attacks - Lacks support for multi host support mechanism
DDoS	Resilient Control Network [42]	Pros: + Minimizes the sharing of critical resources of network + Minimizes the control traffic + Dynamic feedback from each individual node + Makes network more resilient to use
DDoS	Scotah: tool uses overlay based on vSwitch [43]	Pros: + High number of control plane capacity + High data plane capacity to ensure maximum network utilization + Also supports third party integration Cons: - Algorithm learning rate is very low - Perform real time efficiency glitches
DDoS	ANN based algorithm [44]	Pros: + This model is efficient in learning abilities for small samples + It is capable of generalizing from noisy and redundant data Cons: - Algorithm learning rate is very low - Perform real time efficiency glitches
DDoS	Packet Flow Analysis and filtering [45]	Pros: + Reduces the amount of routing traffic + Can predict the network structure change Cons: - Makes network less flexible - Requires a lot of additional resources adding more cost
Jamming	Network Management Protocol [46]	Pros: + Imposes resiliency of network + Reduces the outage rate of end-end communications Cons: - Imposes enhanced utilization of network energy sources - Lacks mobility and other different traffic patterns
Jamming	Network Parameter Analysis [47]	Pros: + Work well with attack detection and mitigation + Provide the fault free services Cons: - Proposed models lacks protocol flexibility - Only works well with the known type of attacks

Table 1. Cont.

Attack Type	SDN-Based Attack Mitigation	Pros and Cons
Clone Attacks	SDN based collaborative RED Protocol [48]	Pros: + Efficient in communication and memory + Improved support for attack detection probability in real time scenarios Cons: - Adds extra overhead to the network
Energy Consumption and Clone Attacks	SDN based Collaborative Rule Enforcement [49]	Pros: + Support for threat detection mechanism + Performs better than other existing approaches for attack detection in efficiency + Robust against communication loss by using multi-path routing scheme Cons: - Latency score for proposed model is low - Adds extra overhead to the network
Spoofing Attack	GPS position finder algorithm [50]	Pros: + Balances the load of nodes and reduces the network congestion + Supports the wireless network mesh & SDN protocols Cons: - No identification of optimal specifications
Spoofing Attack	Node Configuration Restoration [51]	Pros: + This model also prevents the network controller from saturation and cache misses attacks + Enables the system to handle the attack efficiently + Works well only with known definitions of attacks Cons: - Does not work well with attack type detection and mitigation

However, apart from these attacks, DDoS attacks on UAV networks often lead to native device disruptions. DDoS attacks enable adversaries to execute digital update rate attacks on the UAV device [40]. UAV devices equipped with the autopilot options have digitized computers in a way that allows all inputs sent through the UAV network to be discretized. DDoS attacks on UAV networks can be mitigated by using SDN networks. Compared to traditional networks, SDN networks provide network visibility which allows the SDN controller to monitor ongoing network activity and identify instances of DDoS attacks [52]. The additional visibility allows the controllers and switches of SDN to be able to recognize attributes of packet level data being transmitted through the network. As a result, the ability to recognize and classify incoming data packet inputs enables the SDN controller to determine data packet streams in the DDoS attack and can mitigate this attack via traffic offloading or automated blocking of the instances of DDoS attacks [53]. Also, as DDoS attacks usually target the protocol behaviors of UAV devices, the presence of SDN networks in a UAV network identifies DDoS attacks aimed at disrupting protocol behavior and limits the connection aimed at UAV device protocols.

As previously noted [40], due to the separation of the control plane and the data plane, most of the SDN mitigation techniques for DDoS attacks have focused on analyzing network patterns. The technique as advocated by [40] examines network flow patterns to detect abnormal network patterns. To solve such problems associated with poor network performance and network degradation during high network traffic periods, Wang [43] proposes a solution which enables the network to scale up to better control high traffic loads. Scotch, is a tool which uses an overlay based on vSwitch, to allow for elastically scaling up the capacity of SDN control plane. Scotch was designed to utilize take advantage of the high capacity of the data plane. The scalability factor allows the SDN to scale

to increase resilience under abnormal traffic surges such as DDoS attacks as well as under regular traffic surges seen during flash crowds. Moreover, Scotch utilizes the high capacity of the data plane to accommodate a large amount of VSwitches thus enabling it to scale the capacity of SDNs.

Another SDN network mitigation solution focuses on the implementation of machine learning algorithms to provide automated protection against DDoS attacks. The work of [41] leverages a machine learning algorithm to detect a DDoS attack by calculating the entropy of the destination IP address via the SDN controller. A DDoS attack is determined when the entropy value rises above the expected threshold.

The work of [42] also focuses on mitigating DDoS attacks in UAV devices has been proven viable [42]. The authors propose the Resilient Control Network (ReCON) solution, which leverages SDN resources to defend the network's control plane from being affected by DDoS attacks. ReCON seeks to minimize the critical resources shared to control traffic and data flows. Furthermore, ReCON can further elastically increase the limited capacities of all the software control agents. ReCON increases the abilities in real time by using the resources least utilized within the same SDN dynamically. However, to implement and evaluate a practical solution, Gillani [42] designed ReCON as a solution for problems associated with constraint satisfaction through the use of the Satisfiability Modulo Theory. This theory guarantees control plane placement based on an accurate construction which handles any dynamic network changes.

The work of [44] also seeks to leverage machine learning algorithms to better secure the SDN network. The authors use artificial neural networks (ANN) to implement genetic algorithms to make intelligent decisions regarding network traffic. By equipping SDN networks with support vector machine algorithms to allow the network to classify networking traffic using machine learning directly.

Jamming attacks pose a significant threat. Jamming attacks target communication and surveillance components of the UAV device which has implications for the relay of information [54]. For example, jamming attacks are used to perpetrate Automatic Detection Surveillance-Broadcast (ADS-B). An ADS-B attacks components implemented in a UAV is used for navigating UAV devices during the course of a mission. Cyber adversaries use jamming attacks to block an airborne UAV device from communicating with the legitimate control station. Jamming attacks on UAV networks are also able to target the navigational systems and impede their ability to connect to the Global Positioning Systems (GPS) therefore, disrupting critical navigation guidance [55]. This attack also has implications for disrupting the UAV devices ability to operate on autopilot or deliver critical payload information. If an adversary launches a jamming attack to block communication against UAV network, the SDN controller can detect the cause of the disruptions [47]. Seciniti [46] proposed a network management protocol that leverages a multi-layer graph model which can evaluate various communication pathways as a means of enhancing resilience in connectivity. This proposed implementation ensures that UAV devices seeks to increase UAV resilience to jamming attacks.

Another attack that can be perpetrated against UAV devices is cloning attacks. A cloning attack is where an adversaries capture a UAV device operating within the network and reprogram the device. This re-programmes the device and assists in perpetuating additional attacks against the network [48]. This attack can affect additional nodes as membership to the network can allow it access to legitimate pieces of information, therefore aiding in the attack process. Clone attacks require early detection of these affected nodes to secure the network from malicious activities [56]. However, these attacks are crucial in their nature as their existing solutions for these attacks demands more energy resources [57]. Researchers have sought ways to provide early detection of clone devices to ensure secure network reliability [48,56,57].

An early detection mechanism includes the witness-based detection system in which each device is required to send proper identification concerning a set of coordinates, therefore acting as a witness for the device. This solution is based upon the fact that each device should maintain the same identification ID but different positions. When more than one node sends the same ID with different

position information, the clone attack is detected [57–60]. However, these approaches are not as efficient because these devices have limited storage, computational capacity and power resources [57].

Meanwhile, data transfer in more extensive networks requires data aggregation to reduce communication overhead and energy consumption. Roy et al. [49], proposed a loss resilient model named synopsis defusion. Synopsis defusion uses the duplicate insensitive algorithm to aggregate on the top of routing schemes. However, this model lacks the better clone attack as these models do not address the sub-aggregation of malicious nodes in the network under attack. Also, the work of [61] proposes using the programmable open flow switches in the router to allow for more dedicated and secure communication channels. This model enables the nodes to drop the malicious packets by analyzing them to curb the smart adversaries [62].

Cloning attacks in distributed environment where the route for common node and witness node is distributed, ensuring the credibility witness node can be problematic [48]. For distributed networks, Conti et al. [48], proposed a randomized, efficient and distributed protocol for node replication attacks. This protocol starts by identifying the nodes and monitoring its data flow. This protocol randomly decides the witness based of network-wide seeds and the notion that if the adversary knows the location of the witness nodes, then it can subvert security protocols making clone attack detection more challenging [56].

Another proposed solution to mitigate vulnerabilities introduced via malfunctioning devices in the network can be reverted by leveraging SDN. The SDN control plane can detect malfunctioning nodes then transmit the information with respect to the ordinary device nodes over the network [63]. Concerning the solution proposed by [63], the controller detects the node as either disrupting or untrusted and instructs other nodes to cut off communication with the identified device. Apart from this, the SDN controller can also instruct the nodes to ignore the data being transmitted by these cloned nodes in typical ad-hoc environment [63].

Spoofing is a also common attack perpetrated against UAV networks. Spoofing is where input data is manipulated for malicious purposes. For example, spoofing attacks on UAV devices can lead to improper execution of gain scheduling attacks. With this attack, Cyber adversaries can launch scheduled attacks with the intent of gaining complete control of UAV systems. The authors of [64] point out that UAVs require various sensors to perform properly, allowing for full usage of UAVs. Spoofing attacks can also be executed against device functions needed for auto-piloting. These attacks not only impact specific UAV sensor functions but could also impact the UAV as a whole.

SDN-based solutions for mitigation spoofing attacks are used to ensure that sensor activity can continue despite being targeted. The SDN architecture facilitates implementation of storage solutions that support network data to be backed up from the device. Once the UAV device has been targeted, the SDN controller can be programmed to override all the compromised controls using the data from the storage backup [51]. Moreover, the SDN controllers allow for continuous monitoring of UAV networks for signs of spoofing intrusions to allow the deployment of preventive measures to preserve the UAV network before being fully compromised.

In [50], notes that networks are equipped with a GPS position finder algorithms that assist in recovering disabled or disconnected network devices using spatial clustering based on density. The algorithm calculates the most appropriate position of one or more mobile devices are actively deployed, then the affected network connection will be restored within the shortest period. The proposed method also assists in improving communication performance.

7. SDN Enabled UAV Security

Section 7 peels back the layers of SDN enabled UAV security. Section 7.1 speaks to confidentiality attacks on UAV networks. Section 7.2 speaks to integrity attacks on UAV networks. Closing with Section 7.3, which speaks to the availability attacks on UAV networks.

The dynamic nature of UAV network topology makes the security of the SDN system very crucial issue among other key challenges in UAV networks. This section focuses on SDN enabled secure

solutions for UAV networks. To aid in the categorization of the solutions we present the solutions by the following categories: Confidentiality, Integrity, and Availability in the following sections and Table 2.

Table 2. SDN Mitigation Solutions.

SDN Solution Class	SDN Enabled UAV Security Solutions	Pros and Cons
Availability	UAV as a Servi [65]	Pros: + Faster and more efficient coverage area coverage through dense regions area + Simple flow based technique Cons: - Solution requires scale to be truly effective - Solution tested using simulation testing
Availability	Proposed SDN/OODA Networking Architecture [66]	Pros: + Efficient Detection of Denial of Services attacks + Achieves Optimal Network effectiveness Cons: - Imposes an overhead to network usage performance - Also imposes overhead to network access
Availability	Temporospatial Software Defined Networking (TS-SDN) [37]	Pros: + Proactive routing allows for strengthened connections during rapid movement + Maintains topology knowledge of global network (both current and predictive) for increased reliability Cons: - Routing is limited due to the lack of addressing hierarchy - Inability to mitigate against Line-Of-Sight disruptions
Availability	SDN/NFV Integrated Monitoring Architecture [67]	Pros: + Modular mitigation approach allowing for rapid innovation and deployment + Integrates network monitoring tools for real-time device notifications Cons: - Solution effectiveness informed by UAV device limitations - Limited testing data/scenarios for implementation
Availability	SDN/OODA Integrated Platform [68]	Pros: + Efficient Detection of denial of services attacks + Achieves Optimal Network effectiveness Cons: - Imposes an overhead to network usage performance - Also imposes overhead to network access
Availability	Mobility Model for Multi-UAV WSN networks [69]	Pros: + Efficient Detection of denial of services attacks + Achieves Optimal Network effectiveness Cons: - Imposes an overhead to network usage performance - Also imposes overhead to network access
Availability	Large scale UAV nodes in network [70]	Pros: + Controller placement allows for a reduction in network overhead Cons: - Tradeoff exist between the end to end delay and control packet communication overhead

Table 2. Cont.

SDN Solution Class	SDN Enabled UAV Security Solutions	Pros and Cons
Availability	Large scale UAV nodes in network [21]	<p>Pros:</p> <ul style="list-style-type: none"> + Provides energy efficient operations by taking the energy limitations of the nodes into account + Provide prevention of network death routes and failures + Enhances the quality of the video transmissions over the UAV network + Shows better network resilience by enable the nodes to live for longer life. <p>Cons:</p> <ul style="list-style-type: none"> - Shows fluctuation in the percentage of remaining battery for the nodes due to UAV node replacement schemes
Availability	Large scale UAV nodes in network [71]	<p>Pros:</p> <ul style="list-style-type: none"> + Controller placement allows for a reduction in network overhead <p>Cons:</p> <ul style="list-style-type: none"> - Tradeoff exist between the end to end delay and control packet communication overhead
Availability	Multi-tier mesh UAV network [71]	<p>Pros:</p> <ul style="list-style-type: none"> + Provides the multipath TCP communication over the heterogeneous networks + More reliable network in comparison to single path TCP networks regarding the handling of the rapid handoffs in the network + SDN controller is enable to adjust the locations of UAV nodes dynamically + Robust system to handle link congestions and more bandwidth utilization <p>Cons:</p> <ul style="list-style-type: none"> - The proposed solution adds additional overhead for the network to process - adds additional overhead on the network
Availability	Multi-tier heterogeneous UAV networks [72]	<p>Pros:</p> <ul style="list-style-type: none"> + Provides the multipath TCP communication over the heterogeneous networks + More reliable network in comparison to single path TCP networks regarding the handling of the rapid handoffs in the network + SDN controller is enable to adjust the locations of UAV nodes dynamically + Robust system to handle link congestions and more bandwidth utilization <p>Cons:</p> <ul style="list-style-type: none"> - Solution adds additional overhead for the network - adds additional overhead on the network
Availability	Dyna-Q-based reinforcement learning algorithm [73]	<p>Pros:</p> <ul style="list-style-type: none"> + collaborative decision making by using SDN and UAV flight controller + Higher learning rate for the attack detection + collaborative tracking and optimization against jamming attacks <p>Cons:</p> <ul style="list-style-type: none"> - Dyna-Q environment is difficult to build and implement - Adds additional overhead to the network for communication

Table 2. Cont.

SDN Solution Class	SDN Enabled UAV Security Solutions	Pros and Cons
Availability	SDN-Based Secure Mobility Model	<p>Pros:</p> <ul style="list-style-type: none"> + resilient framework against faulty nodes, and intrusion in the network + enhance network throughput and coverage for multiple UAVs + the hybrid model reduces the latency for the UAVs communication <p>Cons:</p> <ul style="list-style-type: none"> - Tradeoff between network coverage and position accuracy
Availability	Hierarchical Detection and Response Scheme [74]	<p>Pros:</p> <ul style="list-style-type: none"> + the models displays high detection rate for large scale UAV network + low number of false positive detections for network traffic + resilient model against grey hole, spoofing and jamming attacks <p>Cons:</p> <ul style="list-style-type: none"> - adds additional overhead and latency into the network - tradeoff between efficiency in energy and security
Availability	SDN/OODA Integrated Platform [68]	<p>Pros:</p> <ul style="list-style-type: none"> + resilient model for false node injection and eavesdropping attacks + only authorized and authentic nodes can join the network + security solutions for major cyber-attacks by means of flexible and programmable central SDN controller in the UAV network <p>Cons:</p> <ul style="list-style-type: none"> - adds additional overhead of node verification and authentication - displays high latency for the UAV nodes' communication
Availability	SD-UAV Networking Architecture which leverages Various Wireless Link Technologies [46]	<p>Pros:</p> <ul style="list-style-type: none"> + adoption of Dijkstra algorithm to assist with calculating diverse paths for optimal routing + efficient model for the reconfiguration of isolated nodes by the means of SDN controller + model treats every node as SDN switch for better reconfiguration and dynamic switching <p>Cons:</p> <ul style="list-style-type: none"> - only consistent with the modern wireless communication standards - adds additional overhead on the network for average end-to-end link outages
Availability	SDN Based Weighted Routing Framework [75]	<p>Pros:</p> <ul style="list-style-type: none"> + resilient model for the network jamming attacks + weighted routing metrics for data flow in the network + resiliency for end-to-end link outages <p>Cons:</p> <ul style="list-style-type: none"> - adds additional overhead for network - adds additional latency for the nodes in the network - tradeoff between latency and efficiency over contemporary competing approaches
Availability	Aerial Network management protocol [46]	<p>Pros:</p> <ul style="list-style-type: none"> + collaborative decision making by using SDN and UAV flight controller + Higher learning rate for the attack detection + collaborative tracking and optimization against jamming attacks <p>Cons:</p> <ul style="list-style-type: none"> - complexity in architecture implementation - adds additional overhead on the network

7.1. Confidentiality Attacks on UAV Networks

The UAV devices allow for the transference of data from the sensors and transmit it towards legitimate/secure control stations. These communication channels can also be directed towards the other UAV devices. However, the data being transmitted should be confidential. This class address the confidentiality of the data to prevent it from malicious users who intend to access it. Malicious actors can reveal the moving orbit information based on the data that they can leak from the active traffic transmissions.

7.2. Integrity Attacks on UAV Networks

Integrity refers to protect the data from being modified or deleted by an unauthorized user. These attacks target the data being transmitted in the UAV network. Device data transmissions differ based upon the mission type. UAV devices which focus on surveillance and other monitoring services are responsible for transferring data to ground control stations. In these attacks, the malicious attackers usually aim to inject the false information or to corrupt the original message.

7.3. Availability Attacks on UAV Networks

This class of attacks usually targets several UAV networking layers specifically the physical and networking layer of the system. Generally, these classes can be understood as those attacks which seek to make the device unavailable for intended purposes. When targeted at the networking layer, the adversary can manipulate the routing protocols and disrupt the network communication by making it disconnected for the devices in the network. Meanwhile, on the physical layer, these attacks can be launched by an attacker to jam and to interfere with the communication channels.

In the above sections, we have defined the classes of solutions to which we leverage in the article. As previously noted, Table 2 presents the SDN enabled solutions for increased security in UAV networks.

Yapp et al. [65] proposed a simulated environment to perform analysis and testing for UAV as a Service integration. They accomplished this by using off-the-shelf frameworks similar to Flight Gear and Ardupilot's Software to simulate real world UAV hardware, in addition to web services and messaging APIs such as RabbitMQ and Java Spring Framework to simulate UAVaaS cloud coordinator and client functionality. The simulation environment was leveraged to conduct further research into the network performance and security issues associated with UAV as a Service configurations. They identified five primary actors who would be interacting with the UAVaaS system: operators, spectators, emergency services personnel, UAV ground crew personnel, and third party UAV vendors.

In the article, Barritt [37] presents an application that operates within UAV networks known as temporal-spatial Software Defined Networking (TS-SDN). As UAVs need wireless communication to allow for an expanded range, reactive repair is relatively costly in comparison to other terrestrial applications, especially when you consider the mechanical considerations for the system. TS-SDN architecture focuses on leveraging proactive routes. Proactive routing allows for programmed pathways to be adjusted in advance of temporary handovers or events that may disrupt a routing path. The ability for routes to be adjusted serves as a mitigation technique if the device or devices experience network attacks. Furthermore, this is a significant advantage as it allows for an increase in availability for the UAV network.

White et al. [67] highlight the centrality of telemetry analysis in UAV link communication. To assist in attack mitigation and network analysis, the authors propose a networking architecture which integrates SDN and Network Function Virtualization (NFV). NFV allows for the development of network-based tools that can aid in securing data communication networks. The authors use configured NFV route traffic based upon routing configuration. When anomalies are detected, functions can be deployed to assist in the mitigation of potential attacks. Furthermore, the platform uses notifications

to enhance the real-time awareness of the platform. Notifications are sent to the pilot if the UAV functionality moves outside of specific predictable ranges.

Mishra et al. [66], proposed integrating oriented Observe, Orient, Decide, and Act (OODA) principals into the SDN controller to allow for improved situational awareness during coalition operations. Coalition operations are operations which involve multiple coalition forces. The authors implement the security situational awareness as a OODA loop in the SDN network. This architecture allows for the integration of multiple military networks to increase collaboration between coalition networks. Within this solution, the OODA loop is responsible for assessing the information and coordinating that information regarding security threats via REST interface. The mitigation ability of this solution is based on its ability to share information regarding UAV network attacks with coalition members. This enhances the ability to mitigate network attacks based upon the sharing of information to reduce vulnerabilities in real time. The proposed architecture allows for integrated insight into attacks via mitigation and attack information shared across the coalition network.

Mishra et al. [68], proposed a model that incorporates the SDN controller as part of the support infrastructure for the network. The nodes that wish to join the network share the credentials for the authentication to keep the network intact from various malicious and false node dissemination attacks. The controller SDN is leveraged in way that it responses quickly with the fed credentials and also provides the security policies for the node and derivations of the operations of the node in the network. The controller is also equipped for the traffic control and routing for the data flow in the network [68].

On the contrary, the node must inform the controller how to gracefully exit the network, to ensure the integrity of the network topology. Furthermore, the rapid change in network topology via the multi-hop communication channels operates dynamically as communication follows between peers and internal nodes. The resilience in these solutions minimizes the impact of complex outages.

Kumar et al. [69], proposed a model that evaluates the density of the network and authenticates the data flow in the network. The proposed model maps the network into a matrix and divides them into sectors. Nodes which fall into a particular section are considered as the default node. A statistical model is then incorporated to determine the controller and the cluster head. The controller is responsible for monitoring the flow of the data for the authentication and coordination of the nodes residing in the network. This novel mobility model is helpful for the way-point secure transmission of the data. Additionally, they were able to enhance the throughput and coverage of the network.

Rehman et al. [70] proposed a scheme aimed at reducing the overhead by control packets. The key finding of this study is that, if the controller is placed in a way that number of hops remains low, the overhead faced by control packets is reduced. However, the author has argued that there exists a tradeoff between the control overhead and end-to-end delay of the packets.

Moradi et al. [71] proposed a framework in which he discussed the network of Evolved Packet Core (EPC) and Radio Access Network (RAN) for UAV. The EPC module consist of the control plane and data plane. The data plane in his proposed framework is responsible for imposing operator policies on the data traffic flow. The direction of flow can be to/from user equipment. However, the control plane is responsible for maintaining key roles such as access control, mobility reconfiguration and security definitions enforcement to prevent the network from several wide spectrum attacks.

Zhao et al. [72] proposed a SDN based framework for special UAV networks such as ships and shore nodes. The author argues that preexisting approach are heavily dependent on the satellite communication which uses the single path TCP for reliable non-interactive data transmission. However, the challenges faced by single path TCP can be resolved by using multipath TCP to improve the overall throughput and reduce the handover delays for the networks. However, the proposed solution uses the centralized SDN controller which uses the OpenFlow on top of it to make the proposed model more robust in response to attacks and security management.

Pu et al. [54], present a multipath routing protocol to allow for more efficient data transmission and increasingly reliable communication. During the occurrence of jamming attacks, in FANETs

the network resiliency is also improved. To differentiate the link qualities between a node and its neighbor nodes, the link quality scheme is proposed by using the statistical information of received signal strength indication of received packets. The authors present an analytical model and its numerical result in terms of RREP packet reception rate of source node. They modify three representative routing protocols, which are dynamic source routing (DSR), optimized link state routing (OLSR), and split multipath routing (SMR), to work in FANETs for performance comparison.

Sedjelmaci et al. [74] advocated for a novel intrusion detection and response system model which detects the network intrusion aimed to undermine the efficiency of the network. The proposed model classifies node behaviors normal, abnormal and malicious behavior. After the node's behavior is organized, the framework incorporates Support Vector Machine (SVM) enables the module to verify the attack detection at the ground station. The author has conducted various experiments to emphasize the simulation results which depict the model's efficiency to detect the attacks on the large scale density of the network [74].

Secinti et al. [46], proposed a hybrid model for the UAV network communication that establishes the SDN framework on the top of the network architecture. Regarding communication, it is increasingly challenging due to multiple interfaces at the current time. The overall directives for the nodes in the network are set by the controller to ensure network integrity. The controller then derives the operations for each node residing on the network while also serving as an SDN switch. To determine if the network was affected, if a node gets isolated or collapses, the controller calculates the most dynamic and flexible routing paths for the data flow. This proposed model also incorporates the OpenFlow 1.5 protocol on each UAV node for quick switching for the dynamic routing based on the flow pattern set by the centralized controller [46].

In another study, Secinti et al. [75] proposed a framework that integrates the SDN controller to ensure robust communication over the UAV network. In this proposed model, the controller develops a connectivity graph of the UAV nodes on the network by leveraging the location coordinates to determine the availability of the node. Once established, the controller calculates the shortest path for the UAV nodes while making sure that every discovered route entails the UAV node had previously connected to an already discovered routing path. This process of route finding is accomplished by the reviewing node participation in relation to routes that operate in a wider networking range.

Zhiwei Li et al. [73] propose a dual framework for solving these smart jamming attacks by using the SDN and UAV. The proposed model works on the collaborative decision making function by using the means of SDN controller and UAV flight controller. These hybrid controller are responsible for collecting the state information about the network which is further used by Dyna Q based reinforcement learning model. This learning model learns about the network state and take decision about the power allocation and derive the defense strategies to mitigate the smart jamming attacks.

Pedro Cumino et al. [21] proposed a hybrid framework using cooperative UAV approach and SDN named as VOEI. VOEI is equipped with decision making by considering the energy limitations of the UAV nodes to prevent the energy related issues of the nodes, network access issues, route failures, and enhances the quality of video transmissions. These operations are done by using the flexibility of the SDN on the top of the nodes architecture to separate the data and control plane thus giving more flexibility and programmability to the network on the fly. VOEI can be very helpful due to the fact that SDN controller takes into account the information of the network to develop more reliable energy routes for better data transmission which is loss pruned in real time. In this framework, the controller is responsible for reliable calculation along with the UAV nodes' backup to keep the network execution smooth even some damage occurs to the network. However, to share the information of the network with the controller, the nodes exchange the control packets with the controller. This exchange of packets can impose additional overhead on the network.

The above solutions seek to highlight the SDN enabled UAV network security solutions which have been used to mitigate network vulnerabilities within the UAV networks. One notable point from our study is that most of the solutions mentioned in our study focused on making this network more

resilient to disruptions. What is clear based upon our study results, is that additional work needs to be done to further explore the SDN architecture and its ability to secure UAV networks outside of its availability. In the next section, we will discuss open issues related to the field of UAV network security.

8. Open Issues and Research Perspectives

In this section, we present some open issues and research perspectives for SDN-based solutions for cyber attacks in UAV networks.

Previous sections show the SDN with its features, UAV networks and SDN based solutions for cyber attacks in UAV networks. However, the proposed integration is the first attempt and is in its early stages, thus creating several opportunities to be addressed before SDN reaches its full potential. SDNs also have some limitations when they are implemented in UAV devices. The limitations and challenges include: difficulty identifying the most appropriate route for UAV devices, SDNs cause frequent link disconnections, UAV devices can be disrupted intentionally, and onboard resources may not be accessed [46]. We discuss key open issues below:

Handling delay and big data. The data produced by UAVs is expected to be huge which is then used to make informed decisions. However, processing of the huge data at resource constrained UAV devices could lead to sub-optimal point or offloading of the huge data to the ground station could lead to extra delay. Thus, a federated framework with context-aware offloading could help reduce delay while handling big data in the proposed architecture.

In an SDN-enabled UAV network, SDN controllers plays a vital role in making decision for the UAV networks. Based on the current state of the art, it is hard to find research work that focuses on integration issues; however, fusion leads to flexible UAV networks while providing robust security.

When a centralized SDN controller is used to make decisions about the UAV networks, the system could suffer from bottleneck or single point of failure. Thus, architecture should incorporate some redundancy to provide fault tolerance. Finding the optimal number of SDN controllers for a given UAV network is worthy of further investigation.

As the usage of UAVs continue to grow, the degree that these devices can operate securely in a populated metropolitan environment that is increasingly becoming connected. Research should continue to explore how SDN technology can assist in ensuring that UAVs can operate securely in a populated metropolitan environment.

Finally, the context-aware offloading schemes should be developed by incorporating machine learning techniques with edge computing for predictive solutions for cyber defense in UAV networks.

9. Conclusions

In UAV networks, communication in UAVs is perhaps the most fundamental property of their diverse use, including civilian and military applications. Ensuring that these UAV devices are capable of securely transmitting data to both UAVs and ground infrastructures, is one of the critical issues. For our study, we have reviewed common cyber-attacks such as DDoS, jamming, device cloning and spoofing and their respective solutions. We have presented different approaches that are available in the state of the art literature and have compared them side-by-side based on their pros and cons in a tabular form. Because of the highly dynamic nature of UAVs and UAV network topology, traditional cyber-defense solutions are not applicable in a straightforward manner. Overall, additional research and development should focus on leveraging the flexibility of the SDN architecture to automate the detection of networking attacks. Of all of the cyber attacks discussed, most of the research has focused on mitigating DDoS attacks. The intersection of machine learning algorithms to mitigate networking attacks has seemed to provide the most promise.

Author Contributions: This survey articles was the result of contributions from all authors more or less equally.

Funding: This work is partly supported by the U.S. National Science Foundation (NSF) under grants CNS 1650831 and HRD 1828811, and by the U.S. Department of Homeland Security (DHS) under grant award number,

2017-ST-062-000003. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies (NSF and DHS).

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

References

1. Rango, A.; Laliberte, A.; Steele, C.; Herrick, J.E.; Bestelmeyer, B.; Schmugge, T.; Roanhorse, A.; Jenkins, V. Using unmanned aerial vehicles for rangelands: current applications and future potentials. *Environ. Pract.* **2006**, *8*, 159–168. [CrossRef]
2. Grodi, R.; Rawat, D.B. UAV-assisted broadband network for emergency and public safety communications. In Proceedings of the 2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Orlando, FL, USA, 14–16 December 2015; pp. 10–14.
3. Rawat, D.B.; Grodi, R.; Bajracharya, C. Enhancing connectivity for communication and control in unmanned aerial vehicle networks. In Proceedings of the 2015 IEEE Radio and Wireless Symposium (RWS), San Diego, CA, USA, 25–28 January 2015; pp. 200–202.
4. Rawat, D.B.; Ghafoor, K.Z. *Smart Cities Cybersecurity and Privacy*; Elsevier: Amsterdam, The Netherlands, 2018.
5. *Unmanned Aircraft System (UAS) Service Demand 2015–2035*; U.S. Air Force: Bedford, MA, USA, 2013.
6. Hartmann, K.; Steup, C. The vulnerability of UAVs to cyber attacks—An approach to the risk assessment. In Proceedings of the 2013 5th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 4–7 June 2013; pp. 1–23.
7. Rani, C.; Modares, H.; Sriram, R.; Mikulski, D.; Lewis, F.L. Security of unmanned aerial vehicle systems against cyber-physical attacks. *J. Def. Model. Simul.* **2016**, *13*, 331–342. [CrossRef]
8. Kim, A.; Wampler, B.; Goppert, J.; Hwang, I.; Aldridge, H. Cyber attack vulnerabilities analysis for unmanned aerial vehicles. In Proceedings of the Infotech@Aerospace 2012, Garden Grove, CA, USA, 19–21 June 2012; p. 2438.
9. Mount, M.; Quijano, E. Iraqi Insurgents Hacked Predator Drone Feeds, U.S. Official Indicates. Available online: <http://edition.cnn.com/2009/US/12/17/drone.video.hacked/index.html> (accessed on 18 December 2009).
10. Arthur, C. SkyGrabber: The \$26 Software Used by Insurgents to Hack into US Drones. *Guardian* **2009**, *17*. Available online: <https://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked> (accessed on 17 December 2019).
11. Rawat, D.B.; Reddy, S.R. Software defined networking architecture, security and energy efficiency: A survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1. [CrossRef]
12. Haleplidis, E.; Pentikousis, K.; Denazis, S.; Salim, J.H.; Meyer, D.; Koufopavlou, O. *Software-Defined Networking (SDN): Layers and Architecture Terminology*; Technical Report; Internet Research Task Force. 2015. Available online: <https://www.rfc-editor.org/info/rfc7426> (accessed on 31 January 2015).
13. Wagner, W. *Lightning Bugs and Other Reconnaissance Drones*; Armed Forces Journal International: Springfield, VA, USA, 1982.
14. Sanders, R. *An Israeli Military Innovation: Uavs*; Technical Report; Industrial College of the Armed Forces: Washington, DC, USA, 2003.
15. Carr, E.B. *Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace*; National Centre for Policy Analysis (NCPA): Dallas, TX, USA, 2013.
16. Newcome, L.R. *Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles*; American Institute of Aeronautics and Astronautics: Reston, VA, USA, 2004.
17. Mahmoud, S.; Mohamed, N. Collaborative UAVs cloud. In Proceedings of the 2014 International Conference on Unmanned Aircraft Systems (ICUAS), Orlando, FL, USA, 27–30 May 2014; pp. 365–373.
18. Jawhar, I.; Mohamed, N.; Al-Jaroodi, J.; Agrawal, D.P.; Zhang, S. Communication and networking of UAV-based systems: Classification and associated architectures. *J. Netw. Comput. Appl.* **2017**, *84*, 93–108. [CrossRef]
19. Oubbati, O.S.; Lakas, A.; Lagraa, N.; Yagoubi, M.B. UVAR: An intersection UAV-assisted VANET routing protocol. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference (WCNC), Doha, Qatar, 3–6 April 2016; pp. 1–6.

20. Scherer, J.; Yahyanejad, S.; Hayat, S.; Yanmaz, E.; Andre, T.; Khan, A.; Vukadinovic, V.; Bettstetter, C.; Hellwagner, H.; Rinner, B. An autonomous multi-UAV system for search and rescue. In Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, Florence, Italy, 18 May 2015; ACM: New York, NY, USA, 2015; pp. 33–38.
21. Cumino, P.; Lobato Junior, W.; Tavares, T.; Santos, H.; Rosário, D.; Cerqueira, E.; Villas, L.; Gerla, M. Cooperative UAV Scheme for Enhancing Video Transmission and Global Network Energy Efficiency. *Sensors* **2018**, *18*, 4155. [\[CrossRef\]](#)
22. Wei, S.; Ge, L.; Yu, W.; Chen, G.; Pham, K.; Blasch, E.; Shen, D.; Lu, C. Simulation study of unmanned aerial vehicle communication networks addressing bandwidth disruptions. In *Sensors and Systems for Space Applications VII: International Society for Optics and Photonics*; SPIE: Bellingham, WA, USA, 2014; Volume 9085.
23. Scott-Hayward, S.; O'Callaghan, G.; Sezer, S. SDN security: A survey. In Proceedings of the 2013 IEEE SDN For Future Networks and Services (SDN4FNS), Trento, Italy, 11–13 November 2013; pp. 1–7.
24. Kreutz, D.; Ramos, F.M.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-defined networking: A comprehensive survey. *Proc. IEEE* **2015**, *103*, 14–76. [\[CrossRef\]](#)
25. MacFarland, D.C.; Shue, C.A. The SDN shuffle: creating a moving-target defense using host-based software-defined networking. In Proceedings of the Second ACM Workshop on Moving Target Defense, Denver, CO, USA, 12 October 2015; ACM: New York, NY, USA, 2015; pp. 37–41.
26. 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. [\[CrossRef\]](#)
27. Jagadeesan, N.A.; Krishnamachari, B. Software-defined networking paradigms in wireless networks: A survey. *ACM Comput. Surv.* **2015**, *47*, 27. [\[CrossRef\]](#)
28. Hadj, S.B.; Rekhis, S.; Boudriga, N.; Bagula, A. A cloud of UAVs for the Delivery of a Sink As A Service to Terrestrial WSNs. In Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media, Singapore, 28–30 November 2016; ACM: New York, NY, USA, 2016; pp. 317–326.
29. Shin, S.; Xu, L.; Hong, S.; Gu, G. Enhancing network security through software defined networking (SDN). In Proceedings of the 2016 IEEE 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, USA, 1–4 August 2016; pp. 1–9.
30. Shu, Z.; Wan, J.; Li, D.; Lin, J.; Vasilakos, A.V.; Imran, M. Security in software-defined networking: Threats and countermeasures. *Mob. Netw. Appl.* **2016**, *21*, 764–776. [\[CrossRef\]](#)
31. Weinstein, S.B. SDN control in a combined sensor, information retrieval, and communications network for dangerous environments. In Proceedings of the 2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), Tel-Aviv, Israel, 13–15 November 2017; pp. 1–5.
32. Caria, M.; Jukan, A.; Hoffmann, M. SDN partitioning: A centralized control plane for distributed routing protocols. *IEEE Trans. Netw. Serv. Manag.* **2016**, *13*, 381–393. [\[CrossRef\]](#)
33. Liyanage, M.; Abro, A.B.; Ylianttila, M.; Gurtov, A. Opportunities and challenges of software-defined mobile networks in network security. *IEEE Secur. Priv.* **2016**, *14*, 34–44. [\[CrossRef\]](#)
34. Shaghaghi, A.; Kaafar, M.A.; Buyya, R.; Jha, S. Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions. *arXiv* **2018**, arXiv:1804.00262.
35. Sasaki, T.; Pappas, C.; Lee, T.; Hoefler, T.; Perrig, A. SDNsec: Forwarding accountability for the SDN data plane. In Proceedings of the 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, USA, 1–4 August 2016; pp. 1–10.
36. Gupta, L.; Jain, R.; Vaszun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1123–1152. [\[CrossRef\]](#)
37. Barritt, B.; Kichkaylo, T.; Mandke, K.; Zalzman, A.; Lin, V. Operating a UAV mesh & internet backhaul network using temporospatial SDN. In Proceedings of the 2017 IEEE Aerospace Conference, Big Sky, MT, USA, 4–11 March 2017; pp. 1–7.
38. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *arXiv* **2018**, arXiv:1803.00680.
39. Lee, S.; Yoon, C.; Lee, C.; Shin, S.; Yegneswaran, V.; Porras, P.A. *DELTA: A Security Assessment Framework for Software-Defined Networks*; NDSS: New York, NY, USA, 2017.

40. Giotis, K.; Argyropoulos, C.; Androulidakis, G.; Kalogeras, D.; Maglaris, V. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. *Comput. Netw.* **2014**, *62*, 122–136. [[CrossRef](#)]
41. Mousavi, S.M.; St-Hilaire, M. Early detection of DDoS attacks against SDN controllers. In Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 16–19 February 2015; pp. 77–81.
42. Gillani, F.; Al-Shaer, E.; Duan, Q. In-design Resilient SDN Control Plane and Elastic Forwarding Against Aggressive DDoS Attacks. In Proceedings of the 5th ACM Workshop on Moving Target Defense, Toronto, ON, Canada, 15 October 2018; ACM: New York, NY, USA, 2018; pp. 80–89.
43. Wang, A.; Guo, Y.; Hao, F.; Lakshman, T.; Chen, S. Scotch: Elastically scaling up sdn control-plane using vswitch based overlay. In Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies, Sydney, Australia, 2–5 December 2014; ACM: New York, NY, USA, 2014; pp. 403–414.
44. Ashraf, J.; Latif, S. Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques. In Proceedings of the 2014 National Software Engineering Conference, Rawalpindi, Pakistan, 11–12 November 2014; pp. 55–60.
45. Kirichek, R.; Vladiko, A.; Paramonov, A.; Koucheryavy, A. Software-defined architecture for flying ubiquitous sensor networking. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017; pp. 158–162.
46. Secinti, G.; Darian, P.B.; Canberk, B.; Chowdhury, K.R. SDNs in the Sky: Robust End-to-End Connectivity for Aerial Vehicular Networks. *IEEE Commun. Mag.* **2018**, *56*, 16–21. [[CrossRef](#)]
47. Bindra, N.; Sood, M. Is SDN the Real Solution to Security Threats in Networks? A Security Update on Various SDN Models. *Indian J. Sci. Technol.* **2016**, *9*. [[CrossRef](#)]
48. Conti, M.; Di Pietro, R.; Mancini, L.; Mei, A. Distributed detection of clone attacks in wireless sensor networks. *IEEE Trans. Dependable Secur. Comput.* **2011**, *8*, 685–698. [[CrossRef](#)]
49. Roy, S.; Conti, M.; Setia, S.; Jajodia, S. Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 681–694. [[CrossRef](#)]
50. Sriramulu, R.K. Constructing Dynamic Ad-hoc Emergency Networks using Software-Defined Wireless Mesh Networks. Master's Thesis, San Jose State University, San Jose, CA, USA, 2018.
51. Afek, Y.; Bremner-Barr, A.; Shafir, L. Network anti-spoofing with SDN data plane. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM 2017), Atlanta, GA, USA, 1–4 May 2017; pp. 1–9.
52. Dharma, N.G.; Muthohar, M.F.; Prayuda, J.A.; Priagung, K.; Choi, D. Time-based DDoS detection and mitigation for SDN controller. In Proceedings of the 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), Busan, Korea, 19–21 August 2015; pp. 550–553.
53. Ali, A.; Cziva, R.; Jouët, S.; Pezaros, D.P. SDNFV-Based DDoS Detection and Remediation in Multi-tenant, Virtualised Infrastructures. In *Guide to Security in SDN and NFV*; Springer: Berlin, Germany, 2017; pp. 171–196.
54. Pu, C. Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks. *IEEE Access* **2018**, *6*, 68472–68486. [[CrossRef](#)]
55. Sliti, M.; Abdallah, W.; Boudriga, N. Jamming Attack Detection in Optical UAV Networks. In Proceedings of the 2018 20th International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 1–5 July 2018; pp. 1–5.
56. Conti, M.; Di Pietro, R.; Spognardi, A. Clone wars: Distributed detection of clone attacks in mobile WSNs. *J. Comput. Syst. Sci.* **2014**, *80*, 654–669. [[CrossRef](#)]
57. Dong, M.; Ota, K.; Yang, L.T.; Liu, A.; Guo, M. LSCD: A low-storage clone detection protocol for cyber-physical systems. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2016**, *35*, 712–723. [[CrossRef](#)]
58. Zheng, Z.; Liu, A.; Cai, L.X.; Chen, Z.; Shen, X.S. Energy and memory efficient clone detection in wireless sensor networks. *IEEE Trans. Mob. Comput.* **2016**, *15*, 1130–1143. [[CrossRef](#)]
59. Lal, A.; Selvakumar, J. Secure low-storage clone detection technique for wireless sensor networks. In Proceedings of the 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 20–22 April 2017; Volume 1, pp. 669–672.
60. Aalsalem, M.Y.; Khan, W.Z.; Saad, N.; Hossain, M.S.; Atiquzzaman, M.; Khan, M.K. A new random walk for replica detection in WSNs. *PLoS ONE* **2016**, *11*, e0158072. [[CrossRef](#)]

61. McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Shenker, S.; Turner, J. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 69–74. [[CrossRef](#)]
62. Sayeed, M.A.; Sayeed, M.A.; Saxena, S. Intrusion detection system based on Software Defined Network firewall. In Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 4–5 September 2015; pp. 379–382.
63. Toso, G.; Munaretto, D.; Conti, M.; Zorzi, M. Attack resilient underwater networks through software defined networking. In Proceedings of the International Conference on Underwater Networks & Systems, Rome, Italy, 12–14 November 2014; ACM: New York, NY, USA, 2014; p. 44.
64. Noble, D.; Bhandari, S. Neural network based nonlinear model reference adaptive controller for an unmanned aerial vehicle. In Proceedings of the 2017 International Conference on Unmanned Aircraft Systems (ICUAS), Miami, FL, USA, 13–16 June 2017; pp. 94–103.
65. Yapp, J.; Seker, R.; Babiceanu, R. UAV as a Service: A Network Simulation Environment to Identify Performance and Security Issues for Commercial UAVs in a Coordinated, Cooperative Environment. In *Proceedings of the International Workshop on Modelling and Simulation for Autonomous Systems, Rome, Italy, 15–16 June 2016*; Springer: Cham, Switzerland, 2016; pp. 347–355.
66. 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; pp. 3–4.
67. White, K.J.; Denney, E.; Knudson, M.D.; Mamerides, A.K.; Pezaros, D.P. 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 2017; pp. 522–527.
68. Mishra, V.K.; Verma, D.C.; Williams, C. Improving Security in Coalition Tactical Environments Using an SDN Approach. In *Guide to Security in SDN and NFV*; Springer: Cham, Switzerland, 2017; pp. 273–298.
69. Kumar, R.; Sayeed, M.A.; Sharma, V.; You, I. An SDN-Based Secure Mobility Model for UAV-Ground Communications. In *Proceedings of the International Symposium on Mobile Internet Security, Jeju Island, Korea, 19–22 October 2017*; Springer: Singapore, 2017; pp. 169–179.
70. Ur Rahman, S.; Kim, G.H.; Cho, Y.Z.; Khan, A. Deployment of an SDN-based UAV network: Controller placement and tradeoff between control overhead and delay. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 18–20 October 2017; pp. 1290–1292.
71. Moradi, M. Software-Driven and Virtualized Architectures for Scalable 5G Networks. Ph.D. Thesis, The University of Michigan, Ann Arbor, MI, USA, 2018.
72. Zhao, Q.; Du, P.; Gerla, M.; Brown, A.J.; Kim, J.H. Software Defined Multi-Path TCP Solution for Mobile Wireless Tactical Networks. In Proceedings of the 2018 IEEE Military Communications Conference (MILCOM 2018), Los Angeles, CA, USA, 29–31 October 2018; pp. 1–9.
73. Li, Z.; Lu, Y.; Shi, Y.; Wang, Z.; Qiao, W.; Liu, Y. A Dyna-Q-Based Solution for UAV Networks Against Smart Jamming Attacks. *Symmetry* **2019**, *11*, 617. [[CrossRef](#)]
74. Sedjelmaci, H.; Senouci, S.M.; Ansari, N. A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. *IEEE Trans. Syst. Man. Cybern. Syst.* **2018**, *48*, 1594–1606. [[CrossRef](#)]
75. Secinti, G.; Darian, P.B.; Canberk, B.; Chowdhury, K.R. Resilient end-to-end connectivity for software defined unmanned aerial vehicular networks. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.