PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks

Mohamad Sbeiti, *Member, IEEE*, Niklas Goddemeier, *Student Member, IEEE*,
Daniel Behnke, *Student Member, IEEE*, and Christian Wietfeld, *Senior Member, IEEE*

***Abstract*—Low-altitude unmanned aerial vehicles (UAVs) combined with WLAN mesh networks (WMNs) have facilitated the emergence of airborne network-assisted applications. In disaster relief, they are key solutions for 1) on-demand ubiquitous network access and 2) efficient exploration of sized areas. Nevertheless, these solutions still face major security challenges as WMNs are prone to routing attacks. Consequently, the network can be sabotaged, and the attacker might manipulate payload data or even hijack the UAVs. Contemporary security standards, such as the IEEE 802.11i and the security mechanisms of the IEEE 802.11s mesh standard, are vulnerable to routing attacks as we experimentally showed in previous works. Therefore, a secure routing protocol is indispensable for making feasible the deployment of UAV-WMN. As far as we know, none of the existing research approaches have gained acceptance in practice due to their high overhead or strong assumptions. Here, we present the position-aware, secure, and efficient mesh routing approach (PASER). Our proposal prevents more attacks than the IEEE 802.11s/i security mechanisms and the well-known, secure routing protocol ARAN, without making restrictive assumptions. In realistic UAV-WMN scenarios, PASER achieves similar performance results as the well-established, nonsecure routing protocol HWMP combined with the IEEE 802.11s security mechanisms.**

***Index Terms*—Wireless mesh networks, secure routing, routing attacks, IEEE 802.11s, IEEE 802.11i, PASER, ARAN, HWMP, BATMAN, unmanned aerial vehicles.**

I. Introduction

The RECENT United Nations' global assessment report on disaster risk reduction [2] reveals an increase in the number of disasters in recent years that result in more severe humanitarian disasters and economic damage. The report indicates that one of the top concerns in disaster areas is the disruption of telecommunications. In this context, Sugino [3] reports, in a summary of the damages of the great east Japan earthquake and tsunami in March 2011, that 1.9 million fixed telephone lines and 29,000 cellular base stations were damaged. He also reveals that emergency restoration of communication networks took one month, while a full restoration took 11 months. These facts emphasize the increasing importance of portable communication networks in disaster areas. Moreover, these figures point out that a communication network that does not rely on existing infrastructure and that can be deployed in a substantially short period (e.g., one hour) is indispensable to efficiently cope with large-scale crises. Low-altitude, autonomous Unmanned Aerial Vehicles (UAVs) acting as WLAN or LTE aerial hotspots meet these requirements [1], [4]. Additionally, the UAVs can be equipped with sensors for cooperative exploration of scenarios where uncontrolled emissions of liquid or gaseous contaminants exist [5]. UAV-assisted applications also include coverage extension/densification [6], precision farming [7], and polar weather monitoring [8]. Nevertheless, for such applications to become a reality, a reliable, auto-configuring, and self-healing wireless backbone network is needed to interconnect the UAVs and to provide a connection to their ground control station, the Internet, and the cellular core network. Wireless Mesh Networks (WMNs) are a good candidate as they have the aforementioned characteristics [9], and they offer a physical air-to-air link for a direct communication between the UAVs. Fig. 1 illustrates how an airborne mesh network consisting of UAVs connected via a WMN (UAV-WMN) can be used to assist in disaster relief operations. As the figure shows, the UAVs build a portable wireless mesh backbone. This backbone offers, on demand, network coverage to legacy mobile WLAN/LTE clients (rescue fighters' devices). It also deals with the transparent delivery of the clients' data as well as the sensor information of the UAVs.

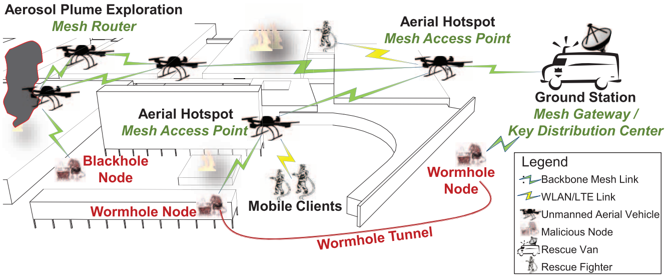


Fig. 1. Example of a deployment scenario of UAV-WMN and two routing attacks in disaster relief.

Manuscript received July 16, 2014; revised February 19, 2015 and July 4, 2015; accepted October 20, 2015. Date of publication November 3, 2015; date of current version March 8, 2016. This work was supported by Deutsche Forschungsgemeinschaft (DFG) within the Collaborative Research Center SFB 876 "Providing Information by Resource-Constrained Analysis", project A4 and has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832 (project SecInCoRe). The text reflects the authors' views. The European Commission is not liable for any use that may be made of the information contained therein. For further information see http://www.secincore.eu/. The associate editor coordinating the review of this paper and approving it for publication was Y. Chen.

The authors are with the Communication Networks Institute (CNI), TU Dortmund University, Dortmund 44227, Germany (e-mail: Mohamad.Sbeiti@tu-dortmund.de; Niklas.Goddemeier@tu-dortmund.de; Daniel.Behnke@tu-dortmund.de; Christian.Wietfeld@tu-dortmund.de).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2015.2497257

A. Problem Statement

While the WMN capability for auto-configuration and self-healing significantly reduces the complexity of the network deployment and maintenance, it makes the WMN backbone prone to routing attacks, including the wormhole and blackhole attacks [10], which are illustrated in Fig. 1. Consequently, an attacker can, with little cost or effort, redirect the traffic and drop the data packets even if the wireless backbone links are encrypted. In UAV-WMN-assisted disaster relief situations, this can sabotage the communication between rescue fighters. In addition, the data exchanged between the UAVs and their ground station will get disrupted. This issue makes the use of WMNs (or any wireless multi-hop solution relying on a routing protocol to dynamically set up routes) problematic for the command and control of the UAVs in practice as flight regulations impose that it should be always possible to remotely pilot the UAVs [11]. Thereby, the control of the UAVs is currently divided into two categories: The high level control of the whole UAV swarm via the operator (the ground station) and the direct control of each UAV via a safety pilot, which burdens pushing UAV-WMN to a wide scale deployment. Apart from that, because the UAVs rely on the exchange of information for autonomous cooperative positioning [5], an attacker might also alter the flight paths of the UAVs by selectively dropping packets. In case the attacker is able to compromise the network credentials and as long as there is no efficient way to refresh those credentials, the attacker might manipulate payload data or even inject corrupted control information that could lead to the highjacking of a UAV. For instance, the attacker might impersonate a UAV and propagate corrupted position information, exploiting the UAVs' collision avoidance mechanisms to indirectly steer UAVs to areas controlled by the attacker. Since the disruption of communications and the violation of the flight security of UAVs can lead to fatal consequences (e.g., near airports), it is vital to deploy a secure UAV-WMN backbone. Two approaches to secure the communication in the mesh backbone exist:

1) Combining well-established, non-secure routing protocols with standardized security mechanisms, such as those of the IEEE 802.11i [12] security standard or the recent IEEE 802.11s [13] mesh standard. However, as we show in [14], [15], these standards are vulnerable to the wormhole and blackhole attacks.
2) Use of a secure mesh routing protocol. Many secure routing protocols have been proposed in the last decade [16], [17], but none of them has been deployed in practice. The high overhead of the security mechanisms of these protocols or the strong assumptions made during their design (e.g., the existence of an efficient symmetric key management scheme) have rendered their deployment in real life applications infeasible.

B. Contributions

A considerable amount of ongoing research dealing with crisis management optimization focuses on the development of a deployable secure mesh routing protocol, such as [18], [19]. This manuscript makes the following noteworthy contributions:

- We present a comprehensive, revised version of the Position-Aware Secure and Efficient Routing approach (PASER) [20], which uses a hybrid cryptosystem and exploits the specifics of UAV-WMN to efficiently secure the routing process.
- We provide a security analysis as well as an extensive performance evaluation of PASER and three representative alternate solutions. ARAN: The well-known, reactive, and secure routing protocol Authenticated Routing for Ad hoc Networks [21]. HWMPS: A combination of the security mechanisms of the IEEE 802.11s mesh standard and the Hybrid Wireless Mesh Protocol (HWMP), which is specified in the mentioned standard. BATMANS: A combination of the IEEE 802.11i security mechanisms and the Better Approach To Mobile Ad hoc Networking (BATMAN) proactive routing protocol [22], which is widely deployed in community networks [23].
  - We analyze the route discovery delay of the protocols in theory and in simulation. We derive lower bound equations of this delay as it constitutes along with the routing overhead, for which we provide asymptotic expressions, the main impact on the overall network performance. The results show that PASER has a more efficient and robust route discovery process than ARAN and BATMANS, and it is scalable with respect to network size and traffic load.
  - Using the network simulator OMNeT++, realistic UAV-mobility patterns, and an experimentally derived channel model, we investigate the performance of the protocols in representative UAV-WMN scenarios under multiple traffic types and various scenario sizes. The results show that PASER mitigates in UAV-WMN more attacks than its alternatives. On top of that, PASER achieves performance comparable to that of HWMPS. This combination of values (security and performance) is deemed to be necessary by the IETF Keying and Authentication for Routing Protocols (KARP) group [24] to drive a broad deployment of a secure routing protocol.

The rest of this paper is organized as follows. We review related work in Section II and highlight the added value of PASER. We present the building blocks of PASER in Section III. A security comparison of PASER and its alternatives with respect to the secure routing needs of UAV-WMN is given in Section IV. Section V provides an extensive performance evaluation of all solutions. The paper closes with a summary of the results in Section VI.

II. Related Work

The surveys in [25]–[27] present a comprehensive analysis of the security in WMNs. They point out that several attacks are common in wireless networks such as jamming at the PHY layer, and these can be mitigated by conventional security mechanisms, while some attacks are specific to WMNs. The latter mainly includes attacks on the core service of the mesh backbone, which is routing, such as the wormhole and blackhole attacks, and user-related attacks, e.g., attacks on the user

TABLE I
SELECTED LIST OF WELL-KNOWN AS WELL AS RECENT SECURE WMN ROUTING PROPOSALS

Protocol name	**Cryptosystem class**	**Main security techniques**	**Deployment impediment in UAV-WMN**
ARAN [21]	Asymmetric-key	Digital signature (PKI)	Computationally expensive on embedded systems [38]
IBC-HWMP [34]		Digital signature (IBC), neighbor monitoring	
IBC/ECDSA-RAOLSR [35]		Digital signature (IBC/PKI-ECC)	
SAODV [36]		Digital signature (PKI), hash chain	
SOLSR [37]		Digital signature (PKI), hash chain, temporal leash	
SWMP [39]		Digital signature (PKI)	
SEAD [40]	Symmetric-key	*MAC*, hash chain, Merkle tree	Interdependency cycle with dynamic key distribution methods [45]
SHWMP [41]		*MAC*, Merkle tree	
SEAODV [42]		*MAC*	
Ariadne [43]	Symmetric-key (or asymmetric)	*MAC* (or digital signature), hash chain	
Castor [44]		*MAC* (or d. s.), Merkle tree, PDR per flow	

ECC: Elliptic Curve Cryptography, IBC: Identity Based Cryptography, PDR: Packet Delivery Ratio, PKI: Public Key Infrastructure

privacy with respect to data content, traffic flows, and location. In this research, we focus on the security of the routing functionality. For privacy preservation and other user-related security services in WMNs, several approaches have been proposed in [28]–[32], which can be applied in combination with secure routing. For instance, in disaster scenarios, end-to-end security mechanisms are already used to ensure the privacy of the data of rescue fighters [33], while the privacy of their traffic flows (source, destination) and their location are not really a concern as these information are predefined in their public regulations.

A list of well-known as well as recent secure WMN routing proposals is depicted in Table I. The proposals are classified according to their cryptosystem. Next, we briefly explore the main security techniques applied in each class, and we highlight common feasibility-related limitations in UAV-WMN.

A. Asymmetric-Key-Based Secure Routing Proposals

In the secure routing proposals, ARAN, SOLSR [37], SAODV [36], and SWMP [39], a Public Key Infrastructure (PKI) is assumed, with each node having a key pair and a certificate. In UAV-WMN, this assumption is feasible as it can be realized by the network operator implementing the certification authority. In IBC-HWMP [34] and IBC-RAOLSR [35], Identity Based Cryptography (IBC) is proposed to avoid the need for a PKI. However many issues in IBC are still unsolved [46], besides, IBC schemes are typically based on Elliptic Curves Cryptography (ECC), which is also used in ECDSA-RAOLSR [35], and the information leaked in 2013 by Edward Snowden revealed that standardized ECC-based algorithms were influenced to include backdoors [47]. Apart from that, due to the complexity of ECC, well known cryptographers have implementation concerns, which could make the system vulnerable despite the security of the algorithm [48]. To guarantee *neighbor authentication*, i.e., to combat the wormhole attack, some approaches (e.g., SOLSR) use temporal leashes [49]. When implementing this approach, all nodes must have accurately synchronized clocks, which is not straightforward in practice. Besides, the scheme does not take into account the channel access delay in UAV-WMN, resulting from CSMA/CA. To minimize the harm of internal attacks, a couple of approaches (e.g., SAODV and SOLSR) include a hop authenticator in the routing messages. They use a hash chain to prevent a malicious intermediate node from decrementing the hop count. However, this scheme is only effective to a small extent, because it can be only used in coordination with the hop count, and the attacker can still forward the message without increasing the hop count. To detect malicious nodes, IBC-HWMP proposes to monitor the behavior of the neighbors. This requires an extra interface in monitor mode, which is very critical in UAV-WMN due to the limited size and weight of the UAVs. Additional limitations of neighbor monitoring are provided in [17].

Deployment impediment in UAV-WMN: This class of secure routing proposals has a high computation time in UAV-WMN, where embedded systems are used [38]. For instance, digital signature operations using RSA-1024 and EDCSA-160 take longer than 26 ms on the Roboard RB110 [50]. This holds for 35 measurements executed using the Linux kernel debugging feature ftrace [51]. Thus, in case of a route with five intermediate hops, the delay is higher than 156 ms. This does not satisfy the quality of user experience of multimedia streaming, where according to [52] the delay should be below 150 ms —Relying on graphical processing units to address this issue does not solve the problem as the parallelism of one digital signature operation comes with the disadvantages of thread synchronization and data exchange overhead [53].

B. Symmetric-Key-Based Secure Routing Proposals

In contrast to the high processing time of asymmetric-key-based secure routing proposals, that of symmetric-key based ones is relatively low. As Table I shows, secure routing proposals of this class mainly rely on *MAC*, hash chains, or/and Merkle trees. That is, they rely on cryptographic hash function-based techniques. With this respect, the cost of SHA-256 on the Roboard RB110 is below 0.15 ms, based on 35 measurements using ftrace and 1500 random bytes. The cost of running 20 iterative calls of SHA-256 is below 0.20 ms. Based on the assumption that the nodes share pairwise secret keys, all the protocols use *MAC* for *message authentication*, either in an end-to-end fashion, such as in Ariadne [43] and Castor [44], or in a hop-by-hop fashion, such as in SEAD [40], SWHMP [41], and SEAODV [42]. To minimize the harm of internal attacks, i.e., to prevent manipulations in the list of forwarding nodes, hash chains are used in SEAD and Ariadne. The security of this mechanism is however limited as it is still vulnerable to manipulations in some cases [54], besides, the attacker can pass the message without adding its identity. Thereby, Merkle trees are additionally used in SEAD. These are integrated in the hash chains to prevent the attacker from passing the routing messages without updating the list of forwarding hops. This approach works well as long as the attacker cannot spoof the identity of legitimate nodes. Merkle trees are used in Castor in a different context. They provide traffic flow authentication. Castor uses the packet delivery ratio of a flow as its security metric. Here, a Merkle tree leaf is appended to each data packet, binding it to a specific flow. The applicability of this approach in UAV-WMN (i.e., at least one CBR traffic flow per UAV) is questionable with respect to the number of trees and leaves needed. In SHWMP, Merkle trees are used in combination with *MAC* and the key scheme of IEEE 802.11s to authenticate the mutable fields in a routing message, in a hop-by-hop fashion. In the authors' opinion, this combination does not improve the security of the protocol as using *MAC* and the key scheme of IEEE 802.11s already leads to one-hop *message authentication*.

Deployment impediment in UAV-WMN: This class of secure routing proposals requires that for every route discovery, the source and destination (and neighbors) must have a security association between them. That is, the existence of a dynamic key distribution method is assumed. This is not straightforward in WMNs [55]. In turn, to dynamically distribute and revoke symmetric keys, secure routes between the nodes are required [45], [46]. Due to the aforementioned deployment impediments of existing secure routing proposals, well-established non-secure routing protocols are combined with the security frameworks of IEEE 802.11s/i (in personal mode) to contemporary reduce the vulnerabilities in current WMN products, see [57], [14]. These frameworks have mainly two problems: First, in personal mode, they are based on static passwords, without supporting a dynamic refresh of the password. Hence, once the attacker compromises the password, the attacker is able to mount all kinds of internal routing attacks, such as the blackhole attack. Second, when using these frameworks, the MAC header of a frame is authenticated but not encrypted. Thus, an external attacker can not change the header but it can read it. Consequently, an external attacker can successfully forward a frame to a legitimate node by manipulating its own MAC address to match that of the frame. This issue can be misused to mount the wormhole attack as shown in [14].

C. Added Value of PASER

With PASER, we strive for a deployable secure routing solution in UAV-WMN. That is, the protocol needs to be feasible, efficient, and it has to be resilient to all relevant routing attacks in UAV-WMN. In this regard, the added value of PASER is threefold.

Hybrid security scheme: PASER implements a sophisticated hybrid cryptosystem, as opposed to the non-hybrid proposals in Table I. Asymmetric cryptography is used for initial mutual authentication and key exchange, after which symmetric cryptography is applied to authenticate the routing messages. Noteworthy with this respect are the two security levels of the symmetric scheme. The first level is based on a group transient key using *MAC*. The second level is based on one-time neighbor authentication tokens using a Merkle tree (a unique use case of Merkle trees). Thereby, even if the attacker compromises the group key and eavesdrops all the messages, the attacker can neither impersonate a legitimate node nor fabricate routing messages as the attacker can not generate new authentication tokens. In contrast, when using the IEEE 802.11s/i security frameworks or symmetric key-based secure routing protocols, once the attacker reveals the key, the attacker can act as a legitimate node. It is shown in [20] that the computational costs of the PASER symmetric scheme is less than 200μ s on the Roboard RB110.

In-band key management method: PASER incorporates an in-band key management method to tackle the interdependency cycle problem between secure routing protocols and key distribution methods [45]. For instance, all the symmetric-key-based proposals in Table I, most of the asymmetric-key-based ones, and the key management method of the IEEE 802.11s/i security frameworks suffer from this problem. In contrast, PASER tackles this issue, allowing for a rapid response to security breaches. This resolves a major issue in current deployments [24]. Noteworthy in this context is the work published in [58], in which it is also proposed to integrate key management and secure routing in one framework, using IBC. While the aforementioned work emphasizes the problem, which we have identified in existing secure routing proposals, it has two drawbacks in comparison to our approach: First, nothing proposed so far solves all the issues of IBC [46]. Second, it uses asymmetric-cryptography in each message.

Specificity to UAV-WMN: PASER exploits the specifics of UAV-WMN, e.g., the network is operated by one organization, and there is a central unit (the ground station), thus, it is appropriate to deploy a PKI and a KDC. Besides, PASER combats a wide range of routing attacks as it aims to fulfill all the secure routing requirements in UAV-WMN, which have been elicited from several research projects, such as [18], [19]. In contrast, the IEEE 802.11s/i and the proposals in Table I are vulnerable to the wormhole or the blackhole attacks, see [14], [17], [26].

III. The Proposed Solution: PASER

PASER aims to secure the routing process in UAV-WMN in a feasible manner. We initially proposed PASER in [20], [59]. In this section, we extend upon our previous works by clearly defining the network and attacker models of PASER, and by extending its security goals, based on discussions with UAV-WMN end-users and stakeholders in [18], [19] among others. Here, PASER has been enhanced to provide *origin authentication* in order to proactively minimize the harm of internal attackers, i.e., to combat the fabrication and blackhole attacks. The *dynamic key management* scheme of PASER has been adjusted to include the key number in all PASER messages for a better detection of key changes. From the routing point of view, the path accumulation has been removed as it was observed that this scheme is ineffective in UAV-WMN. The information gained from path accumulation in UAV-WMN is worth less than the overhead its generates. Apart from that, while we only addressed the route discovery process in our previous works, we have upgraded PASER to include a route maintenance mechanism.

TABLE II
RELEVANT ATTACKS ON UAV-WMN

Type	Class	Name	Description	Consequences
External	Elementary	Time-based replay	Recording routing messages of legitimate nodes and resending these at later times	Building suboptimal routes or route loops
		Position-based replay	Recording routing messages of legitimate nodes and resending them at another location	Building suboptimal routes or route loops
		MAC impersonation	Faking the identity of legitimate nodes using MAC spoofing	Successful processing of attacker frames with respect to identity and delay in case of wireless link encryption
	Compound	Wormhole	*Position-based replay & MAC impersonation:* A pair of attackers, linked via a fast transmission path (tunnel), forward routing messages between two distant nodes	Building of routes that go through the attacker → selective dropping of packets, sabotage of the network, and flight security violation
Internal	Elementary	Flooding	Continuous broadcast of route requests towards non-existing destinations	Consuming network resources such as bandwidth
		Path diversion	Forging routing messages generated by legitimate nodes (e.g., tempering the metric)	Building suboptimal routes or route loops
		IP impersonation	Faking the identity of legitimate nodes using IP spoofing	Generating and propagating corrupted information on behalf of other nodes
		Fabrication (reactive routing only)	Generating forged route replies upon the receipt of route requests; pretending of having optimal routes to destinations	Redirecting and eavesdropping the corresponding traffic → selective dropping of packets
	Compound	Blackhole	*Path diversion & IP impersonation:* Impersonating the main destinations in the network (e.g., mesh gateways) and propagating routing messages with higher sequence numbers and better metrics than the original destinations	Redirecting and eavesdropping the traffic as well as generating and propagating corrupted information → selective dropping of packets, sabotage of the network, flight security violation, and UAV hijacking

A. PASER Assumptions

The PASER approach assumes the following network and attacker models.

1) Network Model: As a target network of PASER, we consider a wireless mesh backbone composed of mobile (UAV) nodes and a static (ground station) node. We assume that the network is operated by one organization (e.g., fire brigades), which restricts the access to the network. Legitimate operator nodes conform to the system protocols while malicious nodes might deviate from them. A public key infrastructure is assumed, with the network operator playing the role of the certification authority. Legitimate nodes have a certificate with integrated roles (gateway, access point, or router). The network operator runs a secure Key Distribution Center (KDC) that is responsible to dynamically manage network credentials. All the nodes know the public key of the KDC. At any time, mesh gateways can establish a reliable connection to the KDC and vice versa. In UAV-WMN, this can be realized by running the KDC at the ground station. It is assumed that the legitimate nodes incorporate a positioning device that runs a secure navigation service, such as the Galileo Public Regulated Service [60]. That is, the target scenario is assumed to be outdoor and to have low obstacles, as in UAV-WMN.

2) Attacker Model: This research focuses on attacks that target the security of routing. The main objective of the attacker is to manipulate the routes in order to sabotage the network or to mount advanced attacks violating the flight security of the UAVs. The attacker is assumed to control a number of external nodes, which might have more power and better communication range than the legitimate nodes. The attacker might also compromise legitimate nodes or network credentials, by means of social engineering, physical attacks, cryptanalysis, and others. Thereby, the attacker can appear in the network as legitimate nodes by utilizing the compromised identities and keys. Nodes under the control of the attacker might arbitrarily deviate from the protocol behavior. In particular, they can drop, modify, or generate corrupted data packets or routing messages. Attacker nodes can also act in coordination, and they can communicate across large distances using additional communication channels. The attacker is, however, computationally bounded and cannot break cryptographic primitives. Table II illustrates the most relevant attacks with respect to our attacker model. A distinction is made between external attacks and internal attacks. In the former case, the attacker has no access to the network. In the latter case, the attacks are performed after revealing network credentials or compromising a legitimate node.

B. PASER Secure Routing Goals

According to the IETF KARP group, it is not only important to provide secure routing proposals but also to deliver deployable solutions (feasible and efficient), see [24]. Since UAV-WMN are closed networks, PASER aims to meet the following three objectives in the order of priority: 1) combating external attacks. 2) dynamically excluding malicious nodes from the network. 3) minimizing the harm of internal attackers until these have been excluded from the network. In other words, PASER strives for establishing and maintaining accurate routes between legitimate nodes. External malicious nodes should not be able to manipulate the routing process or join the network. In case of nodes or key compromise, these nodes should be rapidly excluded from the network, and the keys should be dynamically refreshed. While PASER immediately detects and prevents malicious behavior by which the attacker deviates from the protocol course. The detection of malicious behavior by which the attacker mimics the expected behavior (in case of specific internal attacks, such as path diversion) is not a part of PASER. To this end, a centralized approach running at the ground station might be used. In this way, malicious behavior can be detected based on the deviation of a UAV from its expected behavior and on the anomaly in its key performance indicators. Decentralized detection approaches exist

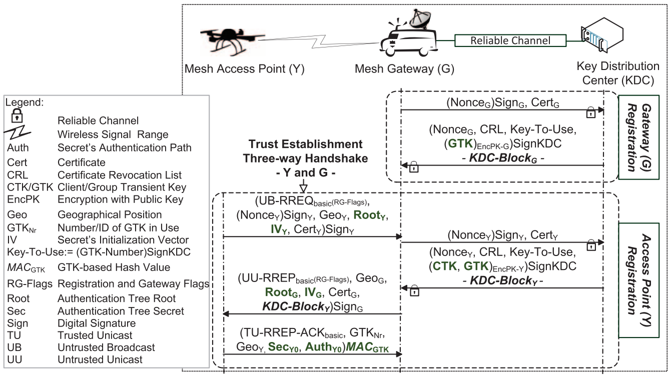

Mesh Access Point (Y)
Mesh Gateway (G)
Reliable Channel
Key Distribution Center (KDC)
Legend:
Reliable Channel
Wireless Signal Range
Auth Secret's Authentication Path
Cert Certificate
CRL Certificate Revocation List
CTK/GTK Client/Group Transient Key
EncPK Encryption with Public Key
Geo Geographical Position
GTK$_{Nr}$ Number/ID of GTK in Use
IV Secret's Initialization Vector
Key-To-Use:= (GTK-Number)SignKDC
MAC_{GTK} GTK-based Hash Value
RG-Flags Registration and Gateway Flags
Root Authentication Tree Root
Sec Authentication Tree Secret
Sign Digital Signature
TU Trusted Unicast
UB Untrusted Broadcast
UU Untrusted Unicast
Trust Establishment Three-way Handshake - Y and G -
(Nonce$_G$)Sign$_G$, Cert$_G$
(Nonce$_G$, CRL, Key-To-Use, (GTK)$_{EncPK-G}$)SignKDC - KDC-Block$_G$ -
Gateway (G) Registration
(UB-RREQ$_{basic(RG-Flags)}$, (Nonce$_Y$)Sign$_Y$, Geo$_Y$, Root$_Y$, IV$_Y$, Cert$_Y$)Sign$_Y$
(Nonce$_Y$)Sign$_Y$, Cert$_Y$
(Nonce$_Y$, CRL, Key-To-Use, (CTK, GTK)$_{EncPK-Y}$)SignKDC - KDC-Block$_Y$ -
(UU-RREP$_{basic(RG-Flags)}$, Geo$_G$, Root$_G$, IV$_G$, Cert$_G$, KDC-Block$_Y$)Sign$_G$
(TU-RREP-ACK$_{basic}$, GTK$_{Nr}$, Geo$_Y$, Sec$_{Y0}$, Auth$_{Y0}$)MAC_{GTK}
Access Point (Y) Registration

Fig. 2. Registration process of nodes and trust establishment between new one-hop neighbors.

as well, such as in [61]. Adopting the honeypot approach [62], used in the botnets field, could be also an attractive solution.

To achieve its secure routing objectives, PASER seeks to fulfill the following security goals: *message authentication*, *message freshness*, *neighbor authentication*, *origin authentication*, and *dynamic key management*.

C. PASER Building Blocks

The PASER secure routing approach comprises three processes: 1) the *node registration process*, which takes place during the network setup and in case of a key refresh. Hereby, all nodes contact the KDC in order to receive the network keys, cf. Fig. 2. 2) the *route discovery process*, which has been adapted from the revised Ad Hoc On-demand Distance Vector protocol (AODVv2) [63] (without path accumulation). 3) the *route maintenance process*, which has been adapted from the NeighborHood Discovery Protocol (NHPD) [64]. Two methods are applied to detect route breaks. First, a link layer feedback mechanism is implemented, which triggers a notification if unicast frames could not be successfully transmitted. Second, nodes periodically broadcast one-hop messages (*Hello*) to monitor trusted one-hop neighbors and to refresh routes to two-hop neighbors. Position information are integrated in the (*Hello*) messages to combat location-based replay attacks, as suggested in [49]. In the following, we elaborate the main operations to secure these processes: a) getting the network security credentials, b) establishing trust between new one-hop neighbors, and c) securing the communication between trusted one-hop neighbors. Afterwards, we describe how PASER refreshes the network key and excludes compromised nodes from the network.

1) Getting Security Credentials From KDC & Establishing Trust Between One-Hop Neighbors: After generating their one-time authentication secrets (Merkle tree leaf pre-image) and computing the root element of the Merkle tree [20], nodes contact the key distribution center in order to join the network. Gateway nodes directly contact the KDC because they have a reliable access to it. Other nodes (routers and access points) first have to look up a route to a gateway in order to reach the KDC. This process is based on the PASER asymmetric scheme, which is illustrated in Fig. 2. To provide *origin authentication*, originator nodes additionally sign non-mutable fields in route requests and replies, such as nonce. After finishing the registration process, a node possesses the required symmetric network keys to successfully operate in the network. The node does not need to contact the KDC to authenticate registered nodes moving in its transmission range. To authenticate registered neighbors, nodes undergo a trust establishment three-way handshake and exchange their position (Geo), Initialization Vector (IV), root element (Root), and certificate (Cert), similar to the handshake between nodes Y and G in Fig. 2, but without the transfer of the *KDC-Block*.

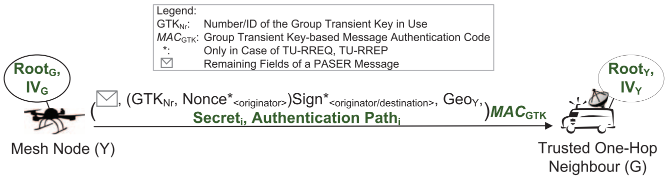

Legend:
GTK$_{Nr}$: Number/ID of the Group Transient Key in Use
MAC_{GTK}: Group Transient Key-based Message Authentication Code
*: Only in Case of TU-RREQ, TU-RREP
✉ Remaining Fields of a PASER Message
Root$_G$, IV$_G$
Root$_Y$, IV$_Y$
(✉, (GTK$_{Nr}$, Nonce*$_{<originator>}$)Sign*$_{<originator/destination>}$, Geo$_Y$, Secret$_i$, Authentication Path$_i$)$MAC_{GTK}$
Mesh Node (Y)
Trusted One-Hop Neighbour (G)

Fig. 3. Symmetric scheme for secure communication between trusted one-hop neighbors.

2) Securing the Communication Between Trusted One-Hop Neighbors: To secure routing messages between trusted one-hop neighbors (e.g., Y and G after the registration), the PASER symmetric scheme is applied, as illustrated in Fig. 3. In this scheme *MAC* is applied on the PASER messages in a hop-by-hop fashion using the Group Transient Key (GTK), which is only known to authorized nodes. Additionally, one-time authentication secrets are included in the messages. A sending node (Y) discloses a secret (Secret$_i$) and sends it along with the corresponding tree path (Authentication Path$_i$) to the next hop (G). Neighbor G, already knowing the IV and root element of Y, verifies if the secret is fresh ($IV_{Secret_i} > IV_Y$). It computes the root of the secret it has received and verifies if it matches the root of Y ($Root(Secret_i, AuthenticationPath_i) = Root_Y$). If true, G can trust that the message has been sent by Y. Consequently, G ensures that the message has been sent by a one-hop neighbor since G only possess the root elements of one-hop neighbors.

3) Key Refreshment and Exclusion of Compromised Nodes: Upon receiving the GTK during the network setup, message originators always include (and sign) the number of the GTK in each PASER message they send (cf. Fig. 2 and Fig. 3). This number is verified at each node that processes the message. In case of a key or node compromise, a key re-generation process is triggered at the KDC, and the certificate of the compromised node is blacklisted. Consequently, a new Key-To-Use mark, the number of the new group transient key signed via KDC: $(GTK_{Nr}^{New})Sign_{KDC}$, is flooded in the network. Upon receiving the new mark, each node resets its routing table and re-registers itself at the KDC, as illustrated in Fig. 2. During this process, legitimate nodes receive the new keys and an updated Certificate Revocation List (CRL), i.e., they get informed about the compromised node. If a legitimate node has not received the reset message due to interference or channel propagation error, it detects from the higher key number in use that a key refreshment has occurred. Its neighbors even proof that by using the new Key-To-Use mark, originated and signed by the KDC.

TABLE III
SECURITY COMPARISON

Comparison of Mitigated Attacks
+: Attack is disabled (proactively), Δ: Attack is prevented (reactively), -: Attack is possible, o: It depends

Attacker type	Attack name	Security goals	PASER	ARAN	HWMPS	BATMANS
External	Internal attacks	Message authentication	+	+	+	+
	Time-based replay	Message freshness	+	+	+	+
	Position-based replay	Neighbor authentication	+	-	-	-
	MAC impersonation	MAC address authentication	-	-	-	-
	Wormhole	Neighbor authentication	+	-	-	-
		MAC address authentication				
Internal	Flooding & path diversion	Intrusion detection & dynamic key management	Δ	o	-	-
	IP impersonation	IP address authentication	o	o	-	-
	Fabrication	Origin authentication	+	+	-	-
		Intrusion detection & dynamic key management				
	Blackhole	IP address authentication	o	o	-	-
		Intrusion detection & dynamic key management	Δ	o		

Comparison of Security Mechanisms

Security goals	PASER	ARAN	IEEE 802.11s/i
Message authentication	Digital signature of forwarder (untrusted neighbors)	Digital signature of forwarder	CCMP
	MAC (trusted neighbors)		
Message freshness	Nonce (untrusted neighbors)	Nonce	CCMP
	Nonce or one-time authentication secrets (trusted neighbors)		
Neighbor authentication	Digital signature and position information of forwarder (untrusted neighbors)	-	-
	One-time authentication secrets and position information of forwarder (trusted neighbors)		
Origin authentication	Digital signature of originator	Digital signature of originator	-
Dynamic key management	Dynamic key management scheme	Broadcast of certificate's revocation	-

CCMP: Counter mode Cipher block chaining Message authentication code Protocol

IV. SECURITY COMPARISON

Table III illustrates a security comparison between PASER, ARAN, HWMPS, and BATMANS with respect to our attacker model. It provides a mapping between each attack and the security goals that must be achieved to combat the attack. It also gives an overview of the mechanisms implemented by each solution to fulfill the security goals. The information provided in the table are based on the analysis in this section and on the works [12]–[14], [20] and [21].

As Table III shows, in case of an external attacker, all solutions protect against the internal and time-base replay attacks as all solutions achieve *message authentication* and *freshness*. Only PASER, however, is able to fulfill *neighbor authentication*. Thus, only PASER protects against the position-based replay and wormhole attacks. This fact is verified in an experimental testbed in [14], [15]. In case of an internal attacker, the IEEE 802.11s/i standards (personal mode) do not provide any protection as the sole credential is the pre-shared key. Once this key is compromised, the attacker can successfully drive all internal attacks, see [14]. In case of ARAN, digital signatures are used to combat the fabrication attack, see Table III. If the IP address of the nodes is bound to their public keys, the digital signature also protects against the impersonation and blackhole attacks. To additionally mitigate internal routing attacks, ARAN implements a broadcasting mechanism of revoked certificates to exclude compromised nodes. ARAN, however, does not address the case of transmission errors of these revocation broadcast messages due to interference or channel errors. In comparison to ARAN, PASER mitigates the same internal attacks and offers a more failsafe *dynamic key management* scheme. PASER guarantees the detection of nodes or key revocation despite non-successful reception of a revocation broadcast message. As long as any neighbor or any node along a requested route between source and destination is aware of the revocation, a PASER node detects it (see Paragraph III-C). In UAV$_{\mathrm{WMN}}$, this is always the case as at least the gateway at the ground station is aware of any revocation process, and this gateway is a common destination for all the UAVs.

V. PERFORMANCE ANALYSIS

To adequately investigate the performance of PASER and its alternatives, the route discovery delay of the protocols is analyzed in theory and in simulation, and asymptotic expressions for the routing overhead are derived. Profiting from the analysis of both factors, we evaluate the protocols' performance using OMNeT++ and INETMANET in a synthetic mobile scenario and two representative UAV-WMN scenarios.

A. Analysis of the Route Discovery Delay

The route discovery delay is composed of the time needed to transmit the required routing messages to find a route, $Cost_{Comm}$, and the time needed to process these messages, $Cost_{Comp}$. The definition of this delay is given in Eq. (1), which is based on the notations in Table IV.

$$Delay_{RD}(D, I^*)_{[s]} = Cost_{Comm(D,I^*)_{[s]}} + Cost_{Comp(D)_{[s]}} \tag{1}$$

Let the route discovery be the case where the sender does not have or lost the routes to the next hop and the corresponding destination, and it needs to (re)discover the latter. Given that

TABLE IV
NOTATIONS USED IN THE ANALYSIS OF THE ROUTE DISCOVERY DELAY

Notation	Description
σ	Estimated average elapsed intervals
$Cost_{Comm}$	Communication costs
$Cost_{Comp}$	Computational costs
D	Diameter: number of links on a route
Dec/Enc	Decryption / encryption
$Delay_{RD}$	Route discovery delay
$Guard_B$	Uniform random time (0, 0.005 s), waited before the transmission of broadcast messages to reduce inter-collision
$I*$	Interval of sending periodic messages; *: only in case of proactive protocols
$MAC_{Gen/Ver}$	Generation / verification of keyed-hash message authentication code
MIC	Message integrity code
Msg, Msg_B, Msg_U	All messages, broadcast messages, unicast messages
$Sign_{Gen/Ver}$	Generation / verfication of digital signature
T_U	Transmission time of unicast frames
T_B	Transmission time of broadcast frames
T_{Op}	Computation time of cryptographic operations
#	Number of

TABLE V
CALCULATION OF LOWER BOUND OF $Cost_{Comm}$ IN EQ. 1

$$Cost_{Comm}(D, I^*)_{[s]} = \sum_{Node=1}^{D+1} (\sum_{i=1}^{\#Msg_B(Node)} (T_B(Size_{Msg})_{[s]} + Guard_{B[s]}) + \sum_{i=1}^{\#Msg_U(Node)} T_U(Size_{Msg})_{[s]}) + \sigma I^*_{[s]}$$

Protocol	Costs [s]
PASER (reactive)	$T_{B_{UB-RREQ}} + Guard_B + (D-1)T_{U_{TU-RREQ}} + (D-1)T_{U_{TU-RREP}}$
ARAN (reactive)	$T_{B_{RREQ_{Sender}}} + Guard_B + (D-1)\ (T_{B_{RREQ_{Inter.}}} + Guard_B)$ $+ T_{U_{RREP_{Destination}}} + (D-1)\ T_{U_{RREP_{Inter.}}}$
HWMPS (reactive part)	$T_{B_{PREQ}} + Guard_B + T_{U_{PREP}}$
BATMANS (proactive)	$1.75\ I + (4+D)\ T_{B_{OGM}} + (4+D)\ Guard_B$

Message sizes of the protocols - Required to calculate T_B and T_U in $Cost_{Comm}$

Message	Size [Byte]	Message	Size [Byte]
		PASER	
UB-RREQ	1066	UU-RREP	1090
TU-RREQ	714	TU-RREP	709
TU-RREP-ACK	538		
		ARAN	
$\text{RREQ}_{\text{Sender}}$	860	$\text{RREQ}_{\text{Intermediate}}$	1693
$\text{RREP}_{\text{Destination}}$	852	$\text{RREP}_{\text{Intermediate}}$	1685
		HWMPS	
PREQ: Path request	27	PREP: Path reply	27
		BATMANS	
OGM: Originator message			16

TABLE VI
CALCULATION OF LOWER BOUND OF $Cost_{Comp_{[s]}}$ IN EQ. 1

$$Cost_{Comp}(D)_{[s]} = \sum_{Node=1}^{D+1} \sum_{Msg=1}^{\#Msg(Node)} \sum_{Op=1}^{\#Op(Msg)} T_{Op_{[s]}}$$

Protocol	Costs [s]
PASER (reactive)	$Nonce_{Gen} + 2Sign_{Gen} + Sign_{Verf} + (D-1)(MAC_{Verf} + MAC_{Gen}) + Sign_{Verf} + Sign_{Gen} + MAC_{Gen} + (D-1)(MAC_{Verf} + MAC_{Gen}) + MAC_{Verf} + Sign_{Verf}$
ARAN (reactive)	$Nonce_{Gen} + Sign_{Gen} + (D-1)Sign_{Gen} + (2D-3)Sign_{Verf} + 2Sign_{Verf} + Sign_{Gen} + (D-1)Sign_{Gen} + (2D-3)Sign_{Verf} + 2Sign_{Verf}$
HWMPS (reactive part)	$2(Enc + MIC_{Add} + Dec + MIC_{Ver})$
BATMANS (proactive)	$(4+D)(Enc + MIC_{Add} + Dec + MIC_{Ver})$

Average time costs of the cryptographic operations in $Cost_{Comp}$ - Measured on a representative embedded system (35 runs)

Cryptographic operation	Time [ms]	PASER	ARAN	HWMPS BATMANS
Signature generation	27.021	x	x	
Signature verification	1.574	x	x	
Nonce generation	0.432	x	x	
MAC generation/verification	0.141	x		
Encryption (hw)	0.089			x
Decryption (hw)	0.072			x
MIC generation/verification (hw)	0.002			x

hw: hardware accelerator

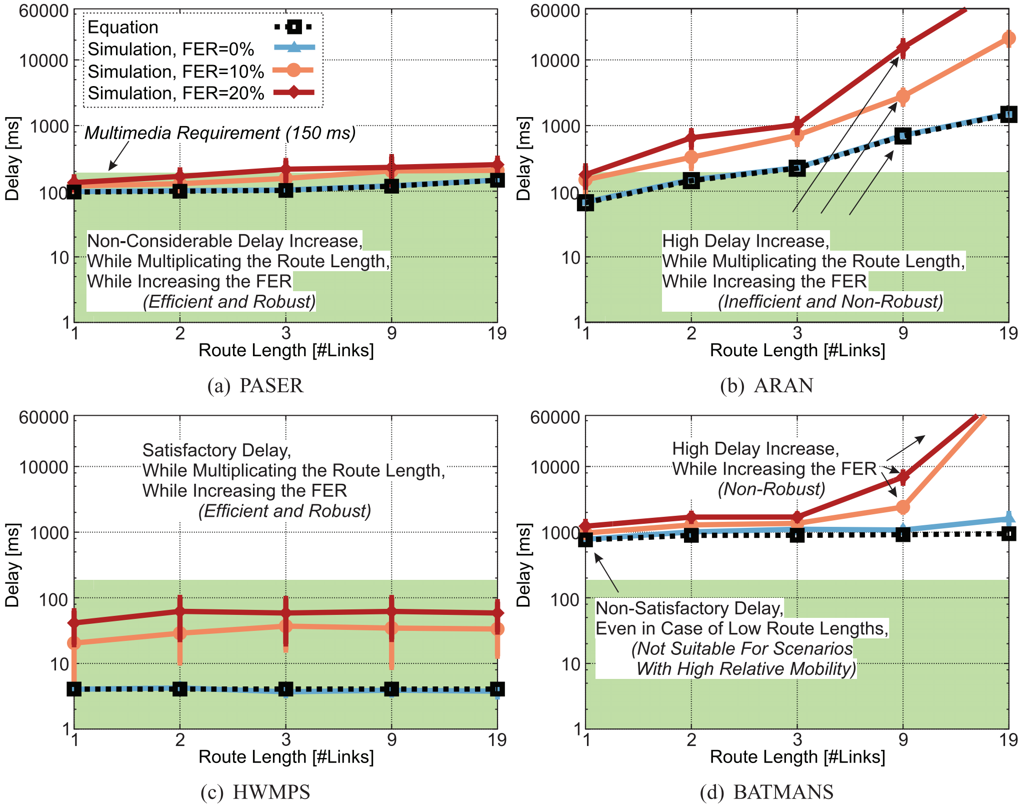
intermediate nodes have the route, a lower bound equation of $Cost_{Comm}$ to find that route is depicted in Table V. In this equation, we assume that the transmission of the routing messages is always successful as our main goal is to compare the efficiency of the security schemes of the protocols when the route length increases, and whether thereby certain latency requirements are violated. Non-successful transmission of the routing messages is dependent on the network topology, traffic load, mobility, and channel characteristics, and it is less related to the security scheme used. It leads to link layer retransmissions and route timeouts, which we investigate using simulation.

As Table V shows, in case of the reactive protocols PASER and ARAN, in contrast to HWMPS, intermediate nodes cannot reply on behalf of the destination due to security reasons. In this respect, PASER mainly relies on unicast messages to contact the destination, while ARAN uses broadcast messages. In case of the proactive protocol BATMANS, at least two periodic messages (called *OGMs*) must be exchanged with the next hop to consider the link as valid. Only then, *OGMs* of the destination received through that next hop are processed. The transmission time of the unicast messages in the equations of Table V can be calculated according to [15].

The transmission time of the broadcast messages can be analogously calculated taking into consideration the use of basic PHY data rates (typically 1 Mbit/s in case of IEEE 802.11g), and that broadcast messages are not acknowledged. The message sizes needed to calculate the transmission time are provided in Table V (bottom). Here, a Merkle tree consisting of 2^{14} secrets, a secret size of 32 Byte, and a certificate size of 701 Byte are assumed.

The equation of $Cost_{Comp}$ to find the route and the time costs of the corresponding cryptographic operations are depicted in Table VI. These costs (see [14], [20] for details about the implementation of the operations) are experimentally measured using ftrace, as in [65], on the Roboard RB110 embedded system, on which a Debian Wheezy with Linux kernel 3.10 is installed. Table VI emphasizes the efficiency of the PASER security scheme as it illustrates that in case the route length increases, efficient *MAC* operations (0.248 ms) are used, i.e., only these depend on the diameter D) while inexpensive signature operations (28.595 ms) are applied in ARAN.

Using Table V and Table VI, the route discovery delay of the protocols can be calculated according to Eq. 1, and it can be determined whether their security schemes are a limitation with respect to latency in large networks. We calculate this delay for route lengths up to 19 links. The IEEE 802.11g technology is



(a) PASER

(b) ARAN

(c) HWMPS

(d) BATMANS

Fig. 4. Time for finding a route to a given destination ($Delay_{RD}$) in theory and in simulation.

considered. The PHY data rate is set to 11 Mbit/s. The basic PHY data rate is 1 Mbit/s. The UDP and IP header sizes are 8 and 20 Byte, respectively. The MAC header size is 34 Byte; in case of HWMPS, it is 38 Byte. The MAC header size is increased by 16 Byte when the IEEE 802.11s/i security mechanisms are used. The BATMANS's *OGM*-interval is set to 0.5 s, according to the findings in [15]. The route discovery delay is also evaluated in the discrete event-based simulation environment OMNeT++ [66] and its INETMANET framework. The latter comprises comprehensive simulation models of standard network protocols as well as the here considered routing protocols. The validity of this framework with respect to practice is shown in [15], [20]. The goal of this simulation-based evaluation is twofold: 1) to validate the derived equations in case of successful transmission of routing messages, and 2) to investigate the impact of non-successful transmissions on the route discovery delay. Here, 10% and 20% unsuccessful transmission rates, i.e., Frame Error Rate (FER), are considered respectively.

Fig. 4 depicts the results of this analysis. As the figure shows, the equations' results match the performance of the protocols in simulation. This attests the validity of these equations. The results show only a slight increase of the route discovery delay of PASER while the route length is multiplied, and the FER is increased. This sheds light on two facts: First, the security scheme of PASER is not a limitation with respect to latency in case of long routes, in contrast to that of ARAN, see Fig. 4 (top right) in case of 0% FER. A comparison of the delay of both protocols given a route length of 19 links highlights the efficiency of the security scheme of PASER, which is ten times faster than ARAN in that case. Second, the route discovery mechanism of PASER, relying on unicast messages, is robust against FER. In contrast, that of ARAN, which relies on broadcast messages to wider propagate the route discovery information, is ineffective in case of high FER. If the messages are not successfully received, they will not be retransmitted, thereby, route timeouts occur, after which a new route request must be started. Fig. 4 (bottom, left) emphasizes the lightweight of HWMPS —At the expense of the security level it can achieve, see Table III. Fig. 4 (bottom, right) indicates that the delay in BATMANS is mainly caused by the periodic message interval as σ intervals ($\sigma \in \mathbb{R}$ *and* $\sigma > 1$) must be waited in order to have exchanged the necessary messages, and in case of high FER, these message can get lost, leading to a considerable increase in the delay. On a final note, while the results in Fig. 4 are generated using IEEE 802.11g, the delay of PASER decreases to more than 20% when using IEEE 802.11n/ac, given route lengths higher than 5 links. That is, by using these recent technologies, PASER is able to meet the multimedia latency requirement of 150 ms [52] even in case of route lengths consisting of 19 links and a FER of 20%.

B. *Asymptotic Message Overhead*

In this section, the message overhead of the routing protocols is estimated as a function of limiting parameters with respect to the network performance, based on the work in [67]. These parameters are the network size N, the average route length L, the average number of one-hop neighbors (node density) Δ, the average number of active routes (traffic flows) per node α, and the mobility (link breakage rate) μ. While the work in [67]

TABLE VII
MESSAGE OVERHEAD OF THE ROUTING PROTOCOLS

Protocol	Broadcast messages rate	Unicast messages rate
PASER	$\mu \cdot \alpha \cdot L \cdot N + h_r \cdot N$	$\Theta(\Delta \cdot \mu \cdot \alpha \cdot L^2 \cdot N)$
ARAN	$\mu \cdot \alpha \cdot L \cdot N \cdot (N-1)$	$\Theta(\mu \cdot \alpha \cdot L^2 \cdot N)$
HWMPS	$\mu \cdot \alpha \cdot L \cdot N + t_p \cdot N$	$\Theta(\Delta \cdot \mu \cdot \alpha \cdot L \cdot N)$
BATMANS	$t_p \cdot N^2$	-

only focused on the overhead of broadcast messages, we also provide an approximation of the overhead of unicast messages as PASER mainly relies on these.

Let h_r be the *hello* rate (i.e., that of PASER) and t_p the topology broadcast rate (i.e., *OGM* rate in case of BATMANS and proactive *PREQ* rate of the root element in case of HWMPS), the message overhead of the routing protocols is illustrated in Table VII. The table depicts the number of messages per second or an asymptotic tight bound of this overhead. This information can be used to support the analysis of the relative performance of the protocols in a certain scenario, as done in Sub-section V-C. It can be also used to determine the scalability of the protocols, using the method proposed in [68]. For instance, let Ohd be the overhead of the protocols and Tr the minimum amount of bandwidth required to forward the traffic load in the network in case the routes were static. Let Ψ_{λ_i} be the network scalability factor with respect to a parameter λ_i and $\rho_{\lambda_i}^{Prot}$ the routing protocol scalability factor, these terms are defined in Eq. 2 and Eq. 3 [68].

$$\rho_{\lambda_i}^{Prot} = \lim_{\lambda_i \to \infty} \frac{\log Ohd^{Prot}(\lambda_1, \lambda_2, \ldots)}{\log \lambda_i} \tag{2}$$

$$\Psi_{\lambda_i} = \lim_{\lambda_i \to \infty} \frac{\log Tr(\lambda_1, \lambda_2, \ldots)}{\log \lambda_i} \tag{3}$$

A protocol is considered scalable with respect to λ_i if $\rho_{\lambda_i}^{Prot} \leq \Psi_{\lambda_i}$. Given a constant Δ in case of an increasing network size [68], [69] and a constant L, it is $MTL(\mu, \alpha, N) = \Theta(\alpha N)$ —Increasing L without bounds would jeopardize the performance of UAV-WMN, on which strict requirements are posed due to critical real-time telemetry transmissions [70]. Thus, $\Psi_{\lambda_\mu} = 0$, $\Psi_{\lambda_\alpha} = 1$, and $\Psi_{\lambda_N} = 1$. Besides, in that case, $Ohd^{PASER} = Ohd^{HWMPS} = \Theta(\mu\alpha N)$, $Ohd^{ARAN} = \Theta(\mu\alpha N^2)$ and $Ohd^{BATMANS} = \Theta(N^2)$. That is, only PASER and HWMPS are scalable with respect to the network size: $\rho_N^{PASER} = \rho_N^{HWMPS} = 1 = \Psi_N < \rho_N^{ARAN} = \rho_N^{BATMANS} = 2$. All the protocols are scalable with respect to the traffic load: $\rho_\alpha^{BATMANS} = 0 < \rho_\alpha^{PASER} = \rho_\alpha^{ARAN} = \rho_\alpha^{HWMPS} = 1 = \Psi_\alpha$. Only BATMANS is scalable with respect to mobility: $\rho_\mu^{BATMANS} = 0 = \Psi_\mu < \rho_\mu^{PASER} = \rho_\mu^{ARAN} = \rho_\mu^{HWMPS} = 1$. Nevertheless, as the relative mobility of low-altitude cooperative UAVs is limited due to their small size and their communication aware mobility strategies (see Paragraph V-C4), the mobility factor is not a major concern in practice. Much more relevant are the network size and the traffic load, for which it has been shown that PASER is scalable.

C. Performance Evaluation

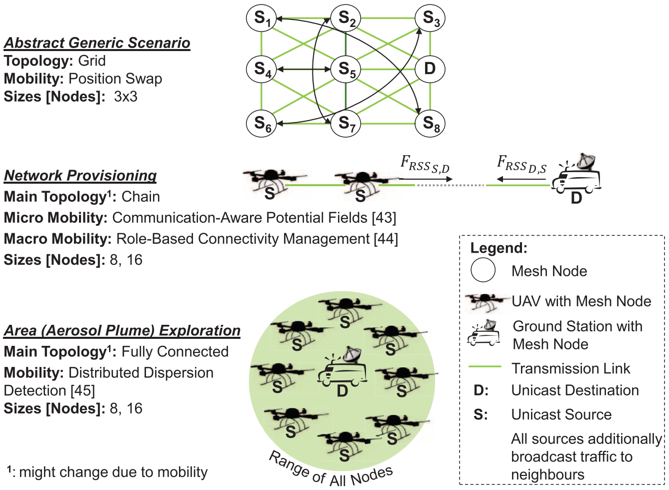

Abstract Generic Scenario
Topology: Grid
Mobility: Position Swap
Sizes [Nodes]: 3x3
S1
S2
S3
S4
S5
D
S6
S7
S8
Network Provisioning
Main Topology¹: Chain
Micro Mobility: Communication-Aware Potential Fields [43]
Macro Mobility: Role-Based Connectivity Management [44]
Sizes [Nodes]: 8, 16
$F_{RSS_{S,D}}$
$F_{RSS_{D,S}}$
S
S
D
Area (Aerosol Plume) Exploration
Main Topology¹: Fully Connected
Mobility: Distributed Dispersion Detection [45]
Sizes [Nodes]: 8, 16
S
D
Range of All Nodes
¹: might change due to mobility
Legend:
Mesh Node
UAV with Mesh Node
Ground Station with Mesh Node
Transmission Link
D: Unicast Destination
S: Unicast Source
All sources additionally broadcast traffic to neighbours

Fig. 5. Overview of analyzed network topologies, traffic flows, and mobility patterns.

In this section, a performance evaluation of the routing protocols in OMNeT++ is presented. First, the corresponding topology and traffic models are outlined. Second, the realistic UAV mobility patterns used, some of which were demonstrated in practice in [18], [19], are elaborated. Third, an experimentally derived channel model for Air-to-Air UAV-WMN links is explored. Afterwards, the results of the performance evaluation are presented.

1) Topology Models: We consider three network topologies, as illustrated in Fig. 5. The first is a grid topology, reflecting a generic synthetic scenario. This topology is used to analyze the impact of link breaks (mobility) and transmission errors on the performance of the protocols. The second is mainly a chain of nodes, representing network provisioning scenarios. It is used to analyze the impact of the route length on the performance. The third is mainly a formation of fully connected UAVs, as intended to be used in aerosol plume exploration scenarios. This topology is used to analyze the impact of the node density on the performance. Different network sizes are investigated, see Fig. 5. For each network size, the transmission range, number and duration of physical links of nodes differs. The available transmission time between any neighbor pair strongly depends on the channel model and mobility patterns used.

2) Traffic Models: We consider two types of traffic, as depicted in Fig. 5. First, broadcast Constant Bit Rate (CBR) traffic is periodically exchanged between neighbor-UAVs, e.g., telemetry data. Second, unicast CBR traffic is sent from all UAVs towards the gateway (the ground station). Depending on the network size, the data rates of both traffic types are adjusted so that the analyzed networks are never congested in case of HWMP (i.e., without security). Hereby, the data rates are set to the maximum value for which HWMP achieves 100% packet delivery in the main topology of each scenario in case all nodes were static.

3) Channel Models: We consider two channel models. The first is a large-scale model based on the free space propagation loss. The second is a combination of the free space model and a small-scale fading model that follows a Rician distribution. The free space propagation loss can be expressed by Eq. 4, with G_t and G_r being the antenna gains, λ the wave length, d the

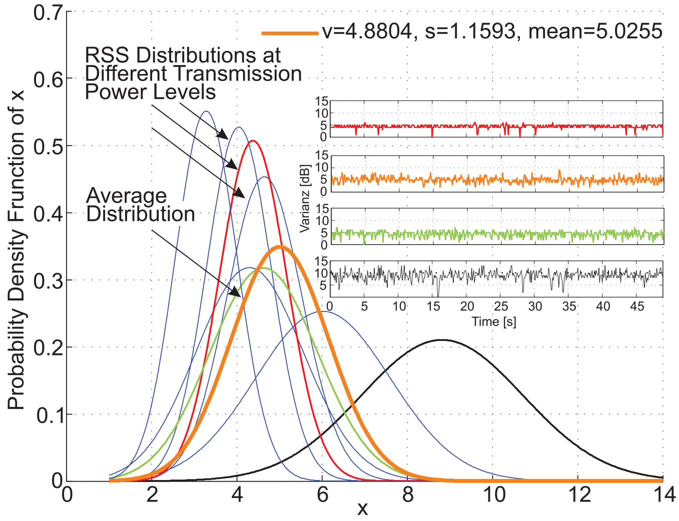


Fig. 6. Parameters identification of Rician channel model for UAV-WMN derived from experiments.

distance between sender and receiver, and γ_0 the attenuation coefficient, see [71].

$$L_{[dB]} = 10\log_{10}\left(\frac{1}{G_t G_r}\left(\frac{4\pi}{\lambda}\right)^2 d^{\gamma_0}\right) \tag{4}$$

The attenuation coefficient γ_0 typically ranges between [2, 5], where $\gamma_0 = 2$ is used for free space (rural) environments, and $\gamma_0 = 5$ is used for (urban) environments with strong damping. Experimental validations of the Air-to-Air UAV-WMN link using two UAVs flying at 30 m altitudes and several WLAN cards such as the DNMA-92 Atheros mini-PCI card and the TP-Link TL-WN821N mini-USB-adapter provided matching results with the free space propagation loss for $\gamma_0 = 2.65$. Therefore, this value is used in this research. The frequency is set to 2.412 GHz, the receiver sensitivity is -91 dBm, the transmitting power is 20 dBm, and $G_t = G_r = 1$. Thus, according to Eq. 4, a node can sense the signal in a range of 473.8 m. The Signal to Noise plus Interference Ratio (SNIR) threshold is set to 4 dB. This means, in case of -101 dBm thermal noise and 9 dB noise factor, as used in this research, the maximum transmission range can be calculated as 365.1 m.

The Rice distribution is defined according to Eq. 5, with $x \in \mathbb{R}_+$, I_0 being the modified Basel function of zero order and the first kind, and v and s reflecting the strength of the dominant and non-dominant paths respectively, see [72].

$$p_\xi(x) = \frac{x}{s^2}\exp\left(\frac{-x^2 - v^2}{2s^2}\right) I_0\left(\frac{xv}{s^2}\right) \tag{5}$$

Through experimental measurements using the hardware-in-the-loop UAV testbed [73], approximations of the parameters v and s are determined. Fig. 6 shows the Probability Density Function (PDF) of x in case of different transmission power levels. Each distribution represents the variation in the Received Signal Strength (RSS) measured by the communication hardware (ranging from -45 dBm to -84 dBm). Based on these results, an average distribution is derived, as depicted in Fig. 6.

TABLE VIII
Link Breakage Rate in the Network Provisioning and Area Exploration Scenarios

Scenario	Network size	Channel type	Link breakage rate μ [Hz]
Network provisioning	8 UAVs	Free Space	$4.3 \cdot 10^{-4}$
	8 UAVs	Rice	$4.4 \cdot 10^{-3}$
	16 UAVs	Rice	$6.1 \cdot 10^{-4}$
Area exploration	8 UAVs	Rice	$5.9 \cdot 10^{-3}$
	16 UAVS	Rice	$3.2 \cdot 10^{-3}$

TABLE IX
Relevant Configurations of Routing Protocols

Parameter	Protocol(s)	Value [s]
OGM-interval	BATMANS	0.5, 1
Hello-interval	PASER	2, 4
PREQ-interval	HWMPS	2, 4
Purge-timeout	BATMANS	5
Neighbor-hold-time	PASER, ARAN, HWMPS	12
Route-hold-time	PASER, ARAN, HWMPS	15

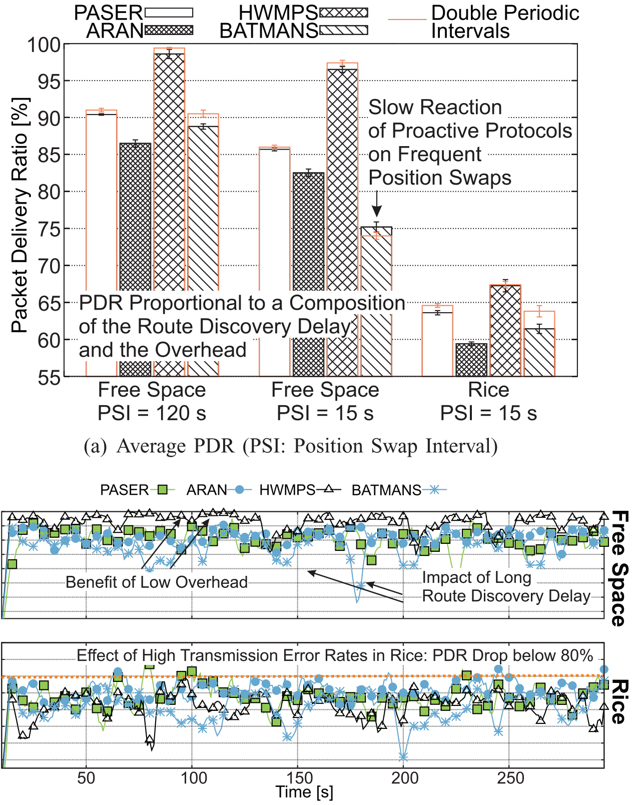
Finally, to obtain a realistic channel model, large-scale and small-scale fading are combined according to Eq. 6, with L_{total} being the total propagation loss.

$$L_{total[dB]} = L_{[dB]} - (p_\xi(x) - mean) \tag{6}$$

4) Mobility Patterns: In the grid scenario, apart from forced position swaps, the nodes are static. The positions of $\text{UAV}_{(N-i) \bmod N}$ and $\text{UAV}_{i \bmod N}$ are swapped each interval i, with N being the number of UAVs in the network. In contrast, in the network provisioning and the area exploration scenarios, nodes moving in three-dimensional space using state-of-the-art mobility algorithms [5] are considered. Each node represents a small-scale UAV flying at altitudes up to 60 m and a maximum speed of 20 m/s. The UAVs' mobility behavior is composed of two components: microscopic mobility which addresses the mobility between the UAVs, and macroscopic mobility strategies, which specifies the locations to which the UAVs travel.

In the network provisioning scenario, the macroscopic location is inherently determined by the users on the ground. In order to extend the coverage area of the UAVs by mean of relaying, a role-based connectivity management scheme (see [5]) is implemented to dynamically reassign the roles of the individual UAVs, based on link monitoring. The microscopic mobility is realized by the communication-aware potential fields (CAPF) algorithm [5], in which virtual potential forces (e.g., F_{RSS}) are calculated based on communication performance indicators (e.g., RSS), cf. Fig. 5. The impact of the mobility on the link breakage rate μ in this scenario is depicted in Table VIII. A link is considered non-reliable or broken if its RSS value is below -83 dBm. As the table shows, the stability of the links in case of 16 UAVs in a 3 km^2 area is higher than that of 8 UAVs in a 2 km^2 area because in the latter case the degree of connectivity and overlapping transmission ranges is lower.

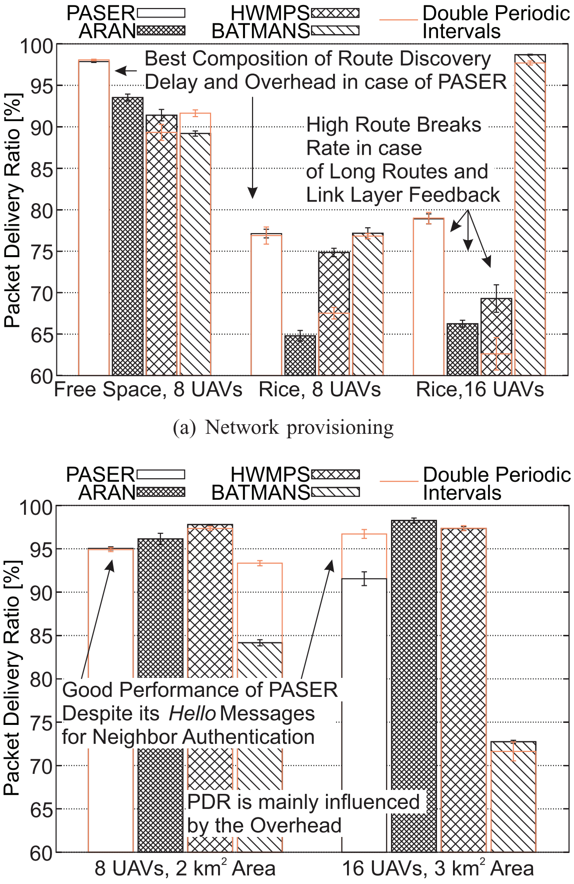
In the aerosol plume exploration scenario, the distributed dispersion detection algorithm [74] is implemented. The UAVs are used to detect the borderline of an aerosol plume. At the same time, the UAVs maintains their communication links to



(a) Average PDR (PSI: Position Swap Interval)

(b) PDR vs. Time, PSI = 15 s

Fig. 7. Packet Delivery Ratios (PDR) in the synthetic grid scenario.



(a) Network provisioning

(b) Radioactive plume exploration - Rice

Fig. 8. Packet delivery ratios in realistic UAV-WMN scenarios.

exchange sensor and telemetry information. The values of μ in this scenario are illustrated in Table VIII. Although the swarm is coherent at all times, frequent changes in the links' quality occurs, due to the highly dynamic behavior of the UAVs. For instance in case of 8 UAVs, approximately one link is broken every eleven seconds: $\frac{1}{\mu \cdot \#Links} = \frac{1000}{5.9 \cdot 15}\, s$. In this regard, the challenge of the routing protocols is to optimally adapt to these changes to avoid packet drops or long delays.

5) Simulation Results: In the following, the performance of the protocols is first analyzed in the synthetic grid scenario. Afterwards, the UAV-WMN realistic scenarios (i.e., network provisioning and area exploration) are considered. In all scenarios, the mobility, channel, and traffic models described in the previous sub-sections are used. The protocols are configured according to Table IX, based on the findings in [15], [75]. Two periodic intervals are considered, and HWMPS is operated in the hybrid registration mode to always have the best route from all nodes to the gateway and vice versa. The simulation time of the grid scenario is 300 s. The simulation time of the network provisioning and area exploration scenarios is 900 s. 35 runs are executed in each case, and a confidence interval of 97.5% is used.

Fig. 7 depicts the Packet Delivery Ratio (PDR) of the protocols in the grid scenario. Both the route discovery time and the message overhead significantly influence the performance in this scenario, cf. Fig. 7(b) (top). HWMPS achieves the best performance, followed by PASER, regardless of the periodic interval's configuration and the Position Swap Interval (PSI), see Fig. 7(a). This is justified by the better composition of the delay and the overhead of both protocols: We showed in Subsection V-A that HWMPS and PASER have a more efficient and robust route discovery process than ARAN and BATMANS, and in this scenario, they also have a lower overhead as $\mu \leq \frac{14}{8} \cdot \frac{1}{300}$ Hz, $\alpha = 1$, $L = 1.5$, $N = 9$, and $\Delta \approx 4.3$, refer to Table IX for the definition of these parameters. Moreover, Fig. 7(a) depicts that in case of a Rician channel, the relative performance of all the protocols but that of ARAN is nearly the same. Fig. 7(b) shows that the maximum PDR in that case is mainly below 80%. Due to fading, the topology (i.e., hidden nodes), and our simulation configuration, many channel errors occur in the Rician channel, which lead to retransmissions of unicast frames, thereby, to more collisions and transmission errors. Here, the better performance of HWMPS and PASER than BATMANS, in contrast to ARAN, attests the efficiency of both protocols, as HWMPS, PASER and ARAN are traffic-aware (i.e., they implement a link layer feedback mechanism), while BATMANS is not.

In the network provisioning scenario, Fig. 8(a) shows that PASER outperforms HWMPS and ARAN. Besides, the performance of PASER gets better in the longer chain of 16 UAVs in case of the Rician channel. As the route discovery delay of PASER is higher than that of HWMPS (cf. Sub-section V-A), and it increases the longer the chain is, the results in Fig. 8 lead to two interpretations: First, the overhead of PASER is lower than that of HWMPS in this scenario. This holds as $\alpha = 1$,

$\Delta \approx 2$, and $\mu < \frac{t_p}{2(L-1)}$. For instance, in case of 8 UAVs, $L = 4$, and $\mu_{FreeSpace} < \mu_{Rice} < \frac{1}{4 \cdot 2 \cdot (4-1)}$ Hz, cf. Table VIII. Second, the chain of 16 UAVs is more stable than that of 8 UAVs. This is true since $\mu_{8-Rice} > \mu_{16-Rice}$, and the overhead of PASER in the latter case is lower as $\frac{\mu_{8-Rice}}{\mu_{16-Rice}} > \frac{L_{16}^2 \cdot 16}{L_8^2 \cdot 8}$ while α and Δ are mainly the same. Apart from these observations, Fig. 8(a) reflects that the longer the route is, and the lower the relative mobility is (i.e., in case of 16 UAVs), the better is the performance of the proactive protocol BATMANS. In that case, the probability of route breaks in case of the reactive protocols is higher. This explains the use of proactive protocols in large community networks.

Due to the high node density in the area exploration scenario, it is the worst-case scenario for PASER. In contrast to the other protocols, PASER fulfills the *neighbor authentication* goal, and it uses, among others, *hello* messages to maintain this goal. For instance, due to the position information in the *hello* messages, when an authenticated one-hop source moves away, and a wormhole attack is mounted at the new location, the destination would detect the attack upon receiving a *hello* message. Otherwise, the nodes would fall in the attacker's trap until the route get lost, due to collision or timeout. The size of the *hello* messages is proportional to Δ as these messages include information about the one-hop neighbors. In this scenario $\Delta \approx N$ since all the nodes are most of the time one-hop neighbors, $D \approx L = 1$. Despite its *hello* messages overhead, Fig. 8(b) shows that PASER can achieve a comparable performance to that of HWMPS in this scenario, given the periodic interval is appropriately set. In contrast, the proactive protocol BATMANS fails to compete in this scenario, especially, at high densities (i.e., 16 UAVs). As the value of μ is below 10^{-2} Hz in this scenario (cf. Table VIII), the overhead of BATMANS is much higher than that of the other protocols, regardless of the periodic interval.

VI. Conclusion

This paper analyzes the PASER secure routing approach in UAV-WMN. It is shown that PASER mitigates —in the investigated scenarios— more attacks than the well-known, secure routing protocol ARAN and the standardized security mechanisms of IEEE 802.11s/i. The efficiency of PASER is explored in a theoretical and simulation-based analysis of its route discovery process, and its scalability with respect to network size and traffic load is reasoned. Using the network simulator OMNeT++, realistic mobility patterns of UAVs, and an experimentally derived channel model of UAV-WMN, it is demonstrated that in UAV-WMN-assisted network provisioning and area exploration scenarios PASER has a comparable performance with that of the well-established, none-secure routing protocol HWMP combined with the IEEE 802.11s security mechanisms. Last, the benefits of PASER were recently presented in different events, such as the Vodafone innovation days 2014 [76], and its implementations in OMNeT++ and in Linux are available under www.paser.info. In future work, we intend to investigate the use of PASER in a broader range of application scenarios.

References

[1] European Commission. (2015). *Flying New Way, RPAS, A Boost for European Creativity and Innovation* [Online]. Available: http://ec.europa.eu/growth/flipbook/rpas/?goback=.gde

[2] United Nations (UN). (2015). *Global Assessment Report on Disaster Risk Reduction* [Online]. Available: http://www.preventionweb.net/english/hyogo/gar/2013

[3] I. Sugino, "Disaster recovery and the R&D policy in Japans telecommunication networks," in *Proc. Opt. Fiber Commun. Conf. Expo./Nat. Fiber Optic Eng. Conf. (OFC/OFOEC)*, 2012.

[4] J. Constine. (2015). *Facebook Will Deliver Internet Via Drones*, TechCrunch [Online]. Available: http://techcrunch.com/2014/03/27/facebook-drones/

[5] C. Wietfeld and K. Daniel, "Cognitive networking for UAV swarms," in *Handbook of Unmanned Aerial Vehicles*, K. P. Valavanis and G. J. Vachtsevanos, Eds. New York, NY, USA: Springer, 2014.

[6] A. Abdulla, Z. Md Fadlullah, H. Nishiyama, N. Kato, F. Ono, and R. Miura, "Toward fair maximization of energy efficiency in multiple UAS-aided networks: A game-theoretic methodology," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 305–316, Jan. 2015.

[7] L. Techy, C. Woolsey, and D. Schmale, "Path planning for efficient UAV coordination in aerobiological sampling missions," in *Proc. IEEE Decision Control (CDC)*, 2008, pp. 2814–2819.

[8] J. Curry, J. Maslanik, G. Holland, and J. Pinto, "Applications of aerosondes in the arctic," *Bull. Amer. Meteorol. Soc.*, vol. 85, no. 12, pp. 1855–1861, 2004.

[9] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, 2005.

[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.

[11] Federal Aviation Administration, U.S. Department of Transportation. (2015). *New Rules for Small Unmanned Aircraft Systems* [Online]. Available: http://www.faa.gov/news/press_releases/news_story.cfm?newsId=18295

[12] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Standard 802.11, 2004.

[13] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11, 2012.

[14] M. Sbeiti and C. Wietfeld, "One stone two birds: on the security and routing in wireless mesh networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2014, pp. 2486–2491.

[15] M. Sbeiti and C. Wietfeld, "The agony of choice: Behaviour analysis of routing protocols in chain mesh networks," in *Proc. Int. Conf. Ad Hoc Netw.*, 2014, vol. 129, pp. 65–81.

[16] H. Y. and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security Privacy*, vol. 2, no. 3, pp. 28–39, May/Jun. 2004.

[17] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 4, pp. 78–93, Jan. 2008.

[18] Airbus Group Innovations (AGI). (2015). *AIRBorne Information for Emergency Situation Awareness and Monitoring* [Online]. Available: http://airbeam.eu/project/

[19] Stadt Dortmund, Feuerwehr. (2015). UAV-Assisted Ad Hoc Networks for Crisis Management and Hostile Environment Sensing [Online]. Available: http://anchors-project.org/index.php/en/

[20] M. Sbeiti, J. Pojda, and C. Wietfeld, "Performance evaluation of PASER—An efficient secure route discovery approach for wireless mesh networks," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, 2012, pp. 745–751.

[21] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated routing for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 3, pp. 598–610, Mar. 2005.

[22] Freifunk Community. (2015). *Better Approach To Mobile Ad hoc Networking* [Online]. Available: http://www.open-mesh.org/

[23] Förderverein Freie Netzwerke e. V. (2015). *Wireless Battle Mesh* [Online]. Available: http://battlemesh.org/AboutUs

[24] G. Lebovitz and M. Bhatia, "Keying and authentication for routing protocols (KARP) design guidelines," RFC 6518. Status: Infomational. Stream: IETF, 2012.

[25] A. Sgora, D. Vergados, and P. Chatzimisios, "A survey on security and privacy issues in wireless mesh networks," *Security Commun. Netw.*,vol. 1, 2013.

[26] J. Sen, "Security and privacy issues in wireless mesh networks: A survey," *CoRR*, vol. abs/1302.0939, 2013.

[27] A. Naveed, S. Kanhere, and S. Jha, "Attacks and security mechanisms," in *Security in Wireless Mesh Networks*, Y. Zhang, J. Zheng, and H. Hu, Eds. New York, NY, USA: Auerbach, 2008.

[28] H. Lin, J. Ma, J. Hu, and K. Yang, "PA-SHWMP: A privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2012, no. 1, 69 pp., 2012.

[29] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 2, pp. 203–215, Feb. 2010.

[30] T. Wu, Y. Xue, and Y. Cui, "Privacy preservation in wireless mesh networks," in *Security in Wireless Mesh Networks*, Y. Zhang, J. Zheng, and H. Hu, Eds. New York, NY, USA: Auerbach, 2008.

[31] X. Wu and N. Li, "Achieving privacy in mesh networks," in *Proc. ACM Security Ad Hoc Sensor Netw. (SASN)*, 2006, pp. 13–22.

[32] Y. Zhang and Y. Fang, "ARSA: An Attack-resilient security architecture for multihop wireless mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 10, pp. 1916–1928, Oct. 2006.

[33] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 619–641, May 2014.

[34] J. Ben-Othman and Y. Saavedra Benitez, "IBC-HWMP: A novel secure identity-based cryptography-based scheme for hybrid wireless mesh protocol for IEEE 802.11s," *Concurr. Comput. Practice Exp.*, vol. 25, no. 5, pp. 686–700, 2013.

[35] Y. Saavedra Benitez, J. Ben-Othman, and J. Claude, "Performance evaluation of security mechanisms in RAOLSR protocol for wireless mesh networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 1808–1812.

[36] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. ACM Workshop Wireless Security (WiSe)*, 2002, pp. 1–10.

[37] F. Hong, L. Hong, and C. Fu, "Secure OLSR," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, 2005, pp. 713–718.

[38] T. Wollinger, J. Guajardo, and C. Paar, "Cryptography in embedded systems: An overview," in *Proc. Embedded World*, 2003, pp. 18–20.

[39] R. Matam and S. Tripathy, "Provably secure routing protocol for wireless mesh networks," *Int. J. Netw. Security*, vol. 16, no. 3, pp. 168–178, 2014.

[40] Y. Hu, D. Johnson, and A. Perrig, "Secure efficient distance vector routing in mobile wireless ad hoc networks," in *Proc. IEEE Workshop Mobile Comput. Syst. Appl. (WMCSA)*, 2002, 31 pp.

[41] M. Islam, M. Hamid, and C. Hong, "SHWMP: A secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks," in *Transactions on Computational Science VI*. New York, NY, USA: Springer, 2009, vol. 5730.

[42] C. Li, Z. Wang, and C. Yang, "Secure routing for wireless mesh networks," *Int. J. Netw. Security*, vol. 13, no. 2, pp. 1–44, 2011.

[43] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *ACM J. Wireless Netw.*, vol. 11, nos. 1–2, pp. 12–23, 2005.

[44] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[45] R. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh, "Bootstrapping security associations for routing in mobile ad-hoc networks," in *Proc. IEEE GLOBECOM*, 2003, pp. 1511–1515.

[46] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 380–400, May 2012.

[47] D. J. Bernstein, T. Lange, and R. Niederhagen. (2015). *Dual EC DRBG, the Basic Back Door* [Online]. Available: https://projectbullrun.org/dual-ec/back-door.html

[48] D. J. Bernstein and T. Lange. (2015). *SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography* [Online]. Available: http://safecurves.cr.yp.to

[49] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE INFOCOM*, 2003, pp. 1976–1986.

[50] DMP Electronics Inc. (2015). *RoBoard RB-110* [Online]. Available: http://www.roboard.com/RB-110.htm

[51] T. Bird, "Measuring function duration with ftrace," in *Proc. Linux Symp.*, 2009, pp. 1–10.

[52] B. Aboba. (2003, Mar.). *Fast Handoff Issues, IEEE 802.11-03/155r0* [Online]. Available: https://mentor.ieee.org/802.11/dcn/03/11-03-0155-00-000i-fast-handoff-issues.ppt

[53] P. Schwabe, "Graphics processing units," in *Secure Smart Embedded Devices: Platforms and Applications*, K. Markantonakis and K. Mayes, Eds. New York, NY, USA: Springer, 2014.

[54] M. Burmester and B. de Medeiros, "On the security of route discovery in MANET," *IEEE Trans. Mobile Comput.*, vol. 8, no. 9, pp. 1180–1188, Sep. 2009.

[55] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," *IEEE Trans. Depend. Secure Comput.*, vol. 2, no. 3, pp. 233–247, Jul./Sep. 2005.

[56] G. Lebovitz, M. Bhatia, and B. Weis, "Keying and authentication for routing protocols (KARP) overview, threats, and requirements," RFC 6862. Status: Infomational. Stream: IETF, 2013.

[57] A. Gerkis. (2014). *A Survey of Wireless Mesh Networking Security Technology and Threats*, SANS Institute [Online]. Available: http://www.sans.org/reading-room/whitepapers/networkdevs/survey-wireless-mesh-networking-security-technology-threats-1657

[58] S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks," *Ad Hoc Netw.*, vol. 11, no. 3, pp. 1046–1061, 2013.

[59] M. Sbeiti, A. Wolff, and C. Wietfeld, "PASER: Position aware secure and efficient route discovery for wireless mesh networks," in *Proc. IARIA SECURWARE*, 2011, pp. 929–934.

[60] European GNSS Agency. (2014). *The Galileo Public Regulated Service—PRS* [Online]. Available: http://www.gsa.europa.eu/security/prs

[61] P.-B. Boek, K. Kohls, D. Behnke, and C. Wietfeld, "Distributed flow permission inspection for mission-critical communication of untrusted autonomous vehicles," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, 2014, pp. 1–6.

[62] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Reading, MA, USA: Addison-Wesley, 2007.

[63] C. Perkins, S. Ratliff, and J. Dowdell, "Dynamic MANET on-demand (AODVv2) routing," Internet-Draft, 2013.

[64] T. Clausen, C. Dearlove, and J. Dean, "Mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP)," RFC 6130. Status: Standards Track. Stream: IETF, 2011.

[65] M. Sbeiti, C. Vogel, A. Wolff, and C. Wietfeld, "ROUTE-O-MATIC: A comprehensive framework for reactive mesh routing protocols," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, 2013, pp. 1151–1155.

[66] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proc. Int. Conf. Simul. Tools Techn. (ICST) SIMUTools*, 2008, pp. 60:1–60:10.

[67] L. Viennot, P. Jacquet, and T. Clausen, "Analyzing control traffic overhead versus mobility and data traffic activity in mobile ad-hoc network protocols," *Wireless Netw.*, vol. 10, no. 4, pp. 447–455, 2004.

[68] C. Santivanez, B. McDonald, I. Stavrakakis, and R. Ramanathan, "On the scalability of ad hoc routing protocols," in *Proc. IEEE INFOCOM*, 2002, pp. 1688–1697.

[69] C. Santivanez, B. McDonald, I. Stavrakakis, and R. Ramanathan, "Making link-state routing scale for ad hoc networks," in *Proc. ACM MobiHoc*, 2001, pp. 22–32.

[70] K. Daniel, A. Wolff, and C. Wietfeld, "Protocol design and delay analysis for a MUAV-based aerial sensor swarm," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2010, pp. 1–6.

[71] H. Friis, "A note on a simple transmission formula," *Proc. IRE*, vol. 34, no. 5, 1946, pp. 254–256.

[72] G. D. Durgin, *Space-Time Wireless Channels*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.

[73] N. Goddemeier, S. Rohde, and C. Wietfeld, "Experimental validation of RSS driven UAV mobility behaviors in IEEE802.11s networks," in *Proc. IEEE GLOBECOM Wi-UAV Workshop*, 2012, pp. 1550–1555.

[74] D. Behnke, P.-B. Boek, and C. Wietfeld, "UAV-based connectivity maintenance for borderline detection," in *Proc. IEEE Veh. Technol. Conf. VTC*, 2013, pp. 1–6.

[75] M. Hiyama, E. Kulla, M. Ikeda, L. Barolli, and M. Takizawa, "Investigation of OLSR behavior for different hello packets intervals in a MANET testbed," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, 2013, pp. 183–188.

[76] M. Sbeiti and D. Behnke. (2015). *Process Oriented, Secure, and Reliable Emergency Group Communication*, Vodafone Innovation Days 2014 [Online]. Available: http://www.kn.e-technik.tu-dortmund.de/images/Forschung/CNI_Vodafone.pdf

Mohamad Sbeiti (M'11) received the Dipl.-Ing. degree in IT security with special focus on applied cryptographic protocols from Ruhr University of Bochum, Bochum, Germany, and the Dr.-Ing. degree from the TU Dortmund University, Dortmund, Germany, in 2009 and 2015, respectively. He joined the Communication Networks Institute (CNI), TU Dortmund University in 2010, as a Research Associate and a Doctoral Student. At CNI, he conducted research and development in the field of secure communication protocols specific to self-organized, interconnected, and wireless networks. He was involved in more than six German and European research projects, which address among other airborne mesh networks, such as AVIGLE and AIRBEAM. He moved to Deutsche Telekom, where he is currently working with the cybersecurity area.

Niklas Goddemeier (S'10) received the Dipl.-Inf. degree in computer science with a major in robotics from TU Dortmund University, Dortmund, Germany, in 2009. During his studies, he worked with the Robotics Research Institute, TU Dortmund, and gained practical experiences in robotics. He currently leads the Networked Robotics Team at the Communication Networks Institute (CNI) of Prof. Christian Wietfeld, TU Dortmund University. He has been actively involved in the research projects such as Airshield, AVIGLE, ANCHORS, and AIRBEAM. His research interests include communication-aware mobility algorithms for UAV swarms.

Daniel Behnke (S'11) received the Dipl.-Inf. degree in computer science from TU Dortmund University, Dortmund, Germany, in 2010. He joined the High Dynamic Networks, Emergency Response Management and Wireless Robotics and 5G Networks research team at the Communication Networks Institute (CNI) as a Research Assistant in December 2010. He coordinates the CNI part in the Franco-German Research Project ANCHORS and contributes to the European FP7 project SecInCoRe. His research interests include robust ad hoc communication and control for unmanned robots in rescue operations.

Christian Wietfeld (M'05–SM'12) received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from RWTH Aachen University, Aachen, Germany. After holding various positions in industry (Siemens, 1997–2005), he joined TU Dortmund University, Dortmund, Germany, in 2005, as a Full Professor and the Head of the Communication Networks Institute. He has authored around 175 peer-reviewed conference papers plus various book chapters, and contributions to standardization and patents. He is currently an Editor for the *IEEE Wireless Communication Magazine* and the *Journal on Emerging Telecommunications Technologies* (Wiley) as well as the Head of the Committee on Communication Networks and Systems in the German Sister Organization of IEEE, ITG. He has had a leading role in several UAV-related research initiatives such as Airshield, AVIGLE, and ANCHORS, and has Co-Founded the IEEE GLOBECOM Wi-UAV workshop on wireless networking of unmanned aerial vehicles. He was the recipient of the Outstanding Contribution Award of ITU-T, in 1999. Since 2008, he has been the recipient of the eight best paper awards (thereof four in IEEE context).