One Stone Two Birds: On the Security and Routing in Wireless Mesh Networks

Mohamad Sbeiti and Christian Wietfeld
Communication Networks Institute (CNI),
Faculty of Electrical Engineering and Information Technology,
Dortmund University of Technology, Germany
Email: {Mohamad.Sbeiti, Christian.Wietfeld}@tu-dortmund.de

***Abstract*—Wireless Mesh Networks (WMNs) have been a major research focus in the recent years leading to a profusion of protocol proposals. While most existing implementations address routing aspects, none of the proposals addressing security aspects have gained acceptance in practice, due to their high overhead or strong assumptions. To cope with security issues in current WMN deployments, well-known non-secure routing protocols such as HWMP, BATMAN or OLSR could be combined with the security frameworks of the IEEE802.11s or the IEEE802.11i standards. In this paper, we analyze the impact of both security frameworks on the performance of WMNs in simulation and in a real testbed. Besides, we experimentally show that both frameworks do not mitigate the blackhole and wormhole attacks. In addition, we demonstrate that an efficient secure routing protocol combined with a dynamic key management scheme are inevitable to establish reliable WMNs.**

I. Introduction

Wireless Mesh Networks (WMNs) have emerged as a key technology to achieve high-performance and low-cost ubiquitous network access in sizeable areas. In emergency operations, WMNs are witnessing an increasing use to establish broadband links to rescue fighters, especially, when infrastructure-based networks fail [1]. Rescue organizations are also willing to use WMNs to interconnect autonomous Unmanned Aerial Vehicles (UAVs) in scenarios where uncontrolled emissions of liquid or gaseous contaminants exist [2]. In the last decade, a profusion of protocols have been proposed to efficiently deploy WMNs and dynamically discover and maintain routes between mesh nodes [3] [4] [5], as well as to secure the network [6], [7]. While many of the routing approaches got mature and are being deployed in practice [8] such as Hybrid Wireless Mesh Protocol (HWMP) [9], Better Approach To Mobile Ad-hoc Networking (BATMAN) [10], and Optimized Link State Routing (OLSR) [11], security has been considered as an afterthought. The deployment of secure WMNs is still facing challenges [12], due to node mobility, their low resources and limited physical protection, and due to the multi-hop wireless communications, which imply a trust in forwarding nodes.

In this paper, we focus on security aspects of WMNs since security is vital to proper operation, and because without a satisfactory level of security, rescue organizations lack motivation to utilize the WMN technology despite its advantages. Many approaches to secure WMNs, especially the routing process, have been proposed so far [6], [7]. However, to the best of the authors‘ knowledge, none of these protocols has been adopted in practice and none of them has a running implementation on the current Linux kernel. The high overhead of the security mechanisms within these protocols or the strong assumptions taken during their design burdened their deployment in real life applications. For instance, Authenticated Routing for Ad-hoc Networks (ARAN) [13], Secure Ad-hoc On-demand Distance Vector (SAODV) [14] and Secure OLSR (SOLSR) [15] are based on asymmetric cryptography, in which every node, originator or intermediate, must sign every message. This provides a high level of security, but it is very expensive with respect to time and energy. We showed in previous work [16] that asymmetric cryptography produces on the Roboard RB110 embedded system (x86 1 GHz, 256 MBytes DRAM) a delay of 70 ms per hop per message. To cope with this overhead issue, Ben-Othman and Benitez propose in [17] to use identity based cryptography, which relies on elliptic curves. It has been shown in [18] that elliptic curves are up to 15 times faster than traditional asymmetric algorithms such as the Rivest, Shamir and Adleman algorithm (RSA). However, Identity based cryptography raises other problems such as the revocation of compromised keys [19]. In contrast to the processing time of asymmetric cryptosystems, that of secure routing messages based on symmetric cryptosystems is relatively low, such as in the secure on-demand routing protocol Ariadne [20], Secure Efficient Ad-hoc Distance vector (SEAD) [21] and Continuously Adapting Secure Topology-Oblivious Routing (CASTOR) [22]. Nevertheless, this class of protocols requires that for every route discovery, the source and destination must have a security association between them. That is, symmetric cryptosystems assume an efficient dynamic key distribution method, which is not straightforward in WMNs.

Thus, as a contemporary solution to combat security issues in current WMN deployments, non-secure routing protocols could be combined with the security frameworks of either the new mesh standard IEEE802.11s [9] (in case of HWMP and other Media Access Control (MAC)-based routing protocols integrated in the IEEE802.11s) or the WLAN security standard IEEE802.11i [23] (in case of BATMAN, OLSR and other IP-based routing protocols). This prevents unauthorized network access and hinders the attacker from injecting, modifying or replaying frames in the network. As only few works [24], [25] have addressed the performance overhead of the IEEE802.11 security frameworks in WMNs, especially, with respect to the new mesh standard, we evaluate both frameworks in static and mobile chain mesh networks. In addition, we experimentally analyze the impact of routing attacks on a WMN secured using those security frameworks to verify whether they can be used to establish reliable WMNs or not. Besides, we investigate if a comprehensive solution that combines efficient secure routing with a dynamic key management scheme such as in Position Aware Secure and Efficient mesh Routing (PASER) [16] is an appropriate alternative to secure WMNs' backbone. In other words, this paper investigates whether combining existing non-secure routing protocols with the security frameworks of IEEE802.11s/i is an appropriate solution to achieve an acceptable trade-off between performance and security in WMNs or whether more work should be devoted to design an alternate proposal.

II. IEEE802.11s and IEEE802.11i Security Frameworks' Overheads

In this section, we analyze the overhead of the security frameworks of IEEE802.11s/i. These comprise two modes of operations, namely, the personal and the enterprise mode. While the personal mode is based on a pre-shared key to access the network, the enterprise mode requires an authentication server to determine whether a node is authorized to access the network by examining the node's credentials. It has been shown in [25], [26], [27] that the enterprise mode is not suitable for dynamic and mobile WMNs, due to high authentication delay values and because there is no permanent reliable link to the authentication server in such environments. Thus, we focus in this work on the personal mode. Establishing a secure session in this mode mainly comprises two phases: The *authentication & key derivation* phase and the *protected data transfer* phase.

A. Delay of Authentication & Key Derivation

This phase necessitates the two-time trigger of the 4-way handshake to mutually authenticate two nodes in case of IEEE802.11i. This process corresponds to the exchange of eight messages [24]. The security framework of the new mesh standard IEEE802.11s requires the same number of message exchanges to that of IEEE802.11i. Figure 1 illustrates the authentication process of IEEE802.11s. Establishing a secure session in the IEEE802.11s standard is based on two protocols, the Simultaneous Authentication of Equals (SAE) and the Authentication Mesh Peering Exchange (AMPE).

- *SAE* is a password-based authentication protocol that relies on elliptic curves and a zero knowledge proof of the password. In contrast to the handshake mechanism of IEEE802.11i, SAE is resilient to offline dictionary attacks [9].
- *AMPE* is responsible for establishing a security association between nodes. That is, its responsibilities/functions include the reaching an agreement on security parameters among nodes and the exchange of group keys.

The delay of the IEEE802.11 security frameworks in this phase mainly comprises, the processing time of the security operations and the transmission time of the security messages. The processing time of relevant security operations measured on the Roboard RB110 embedded system using *ftrace* [28] is provided in Table I. The transmission time mainly depends on the message size and the PHY data rate used. Table II gives the size of relevant messages in both frameworks. The transmission delay of these messages can be calculated according to the equations in Table III. With $T_{<\text{message}>}$ denoting the transmission time of a message, the authentication delay of the security frameworks is given in Table IV. For instance, in case IEEE802.11g is used as a reference communication technology with 11 Mbit/s is set as PHY data rate and 1 Mbit/s as basic PHY data rate, the delays of the mutual authentication of two nodes are:

- $\text{Delay}_{\text{Authentication }_{802.11s}} = 9.04$ ms
- $\text{Delay}_{\text{Authentication }_{802.11i}} = 7.27$ ms

Note that we did not consider key derivation time costs as key derivation can be run in parallel to the message exchange process. Note also that the delay values above are minimum values as additional delay may arise in case of transmission errors or in case of overloaded channels. Besides, these delay values only correspond to one hop link, the multi-hop case is analyzed in the next section.

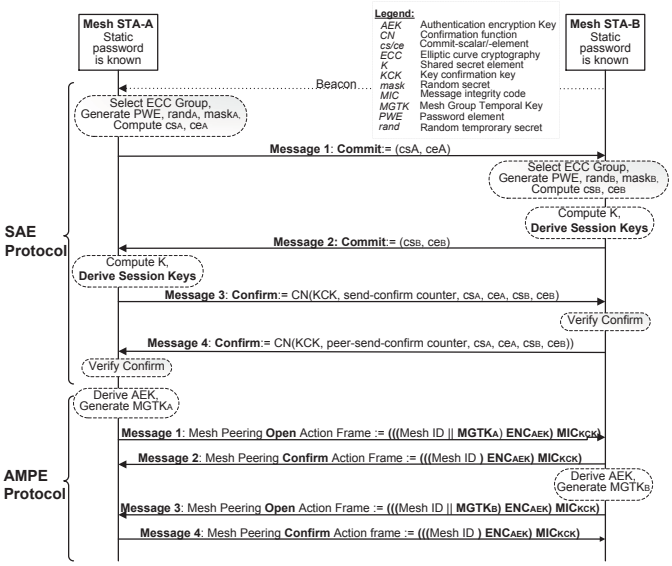

Fig. 1. Establishing a secure session in IEEE802.11s.

TABLE I
AVERAGE PROCESSING TIME OF SECURITY OPERATIONS (10 RUNS).

IEEE802.11s/i	Time [μs]	IEEE802.11s	Time [μs]
Encryption	89.28	Construction of Commit	237.45
Decryption	72.10	Processing of Peer's Commit	211.45
Random Generation	60.42	Construction of Confirm	142.96
MIC add/verify	1.73	Processing of Peer's Confirm	72.62

TABLE II
ORIGINAL SIZE OF RELEVANT SECURITY FRAMEWORKS' MESSAGES.

IEEE802.11s Messages	Size [Bytes]	IEEE802.11i Messages	Size [Bytes]
SAE Commit	104	Handshake Message 1	95
SAE Confirm	40	Handshake Message 2	117
AMPE Open	172	Handshake Message 3	151
AMPE Confirm	172	Handshake Message 4	95

TABLE III
THEORETICAL THROUGHPUT OF IEEE802.11.

$\text{Throughput}_{\text{Basic}}$ =	$\frac{\text{Size}_{\text{Packet}}}{\text{T}_{\text{Transmission}_{\text{Basic}}}}$
$\text{Throughput}_{\text{Basic+Security}}$=	$\frac{\text{Size}_{\text{Packet}}}{\text{T}_{\text{Transmission}_{\text{Basic}}}+\text{T}_{\text{Processing}_{\text{Sender}}}}$
$\text{T}_{\text{Transmission}_{\text{Basic}}}$ =	$\text{DIFS} + \frac{\text{CWmin}\cdot\text{T}_{\text{Slot}}}{2} + \text{T}_{\text{Data}} + \text{SIFS} + \text{T}_{\text{ACK}}$
T_{Data}=	$\frac{\text{PHYHeader}}{1\text{ Mbit/s}} + \frac{(\text{Size}_{\text{Packet}}+\text{UDPHeader}+\text{IPHeader}+\text{MACOverhead})}{\text{Bitrate}}$
T_{ACK}=	$\frac{\text{PHYHeader}}{1\text{ Mbit/s}} + \frac{\text{ACK}}{\text{BasicBitrate}}$
$\text{T}_{\text{Processing}_{\text{Sender}}}$ =	$\text{T}_{\text{encrypt}}+\text{T}_{\text{add}_{\text{MIC}}}=91.01\mu$s

IEEE802.11g Selected Parameter Values.

T_{Slot}	SIFS	DIFS	CWmin
9μs	10μs	28μs	31
UDPHeader	IPHeader	MACOverhead	PHYHeader [bits]
160bits	160bits	272bits	20 (ERP-OFDM), 192 (DSSS)
ACK	RTS	CTS	BasicRateSet [Mbit/s]
112bits	160bits	112bits	1

B. Throughput Overhead of Protected Data Transfer

To guarantee the confidentiality and integrity of data frames, the IEEE802.11 security frameworks rely on the Counter Cipher Mode with Block Chaining Message Authentication Code protocol (CCMP). CCMP expands the original MAC

TABLE IV
AUTHENTICATION DELAYS OF IEEE802.11 SECURITY FRAMEWORKS.

IEEE802.11s	
$Delay_{Authentication_{802.11s}}$ =	$2\cdot(T_{SAEcommit}+T_{construct+process_{SAEcommit}}+T_{SAEconfirm}+T_{construct+process_{SAEconfirm}}+T_{AMPEopen}+T_{processing_{AMPEopen}}+T_{AMPEconfirm}+T_{processing_{AMPEconfirm}})$
$T_{construct+process_{AMPEopen}}$ =	$2\cdot T_{generate_{nonce}}+T_{encrypt}+T_{decrypt}+T_{add_{MIC}}+T_{verfiy_{MIC}}$ =285.05μs
$T_{construct+process_{AMPEconfirm}}$ =	$T_{generate_{nonce}}+T_{encrypt}+T_{decrypt}+T_{add_{MIC}}+T_{verfiy_{MIC}}$ =224.85μs
IEEE802.11i	
$Delay_{Authentication_{802.11i}}$ =	$2\cdot(T_{auth.\ request}+T_{auth.\ reply}+T_{msg.1}+T_{construct+process_{msg.1}}+T_{msg.2}+T_{construct+process_{msg.2}}+T_{msg.3}+T_{construct+process_{msg.3}}+T_{msg.4}+T_{construct+process_{msg.4}})$
$T_{construct+process_{msg.1}}$ =	$T_{generate_{nonce}}$ =60.2μs
$T_{construct+process_{msg.2}}$ =	$T_{generate_{nonce}}+T_{add_{MIC}}+T_{verfiy_{MIC}}$ =63.55μs
$T_{construct+process_{msg.3}}$ =	$T_{encrypt}+T_{add_{MIC}}+T_{verfiy_{MIC}}+T_{decrypt}$=164.65$\mu$s
$T_{construct+process_{msg.4}}$ =	$T_{add_{MIC}}+T_{verfiy_{MIC}}$=3.35$\mu$s

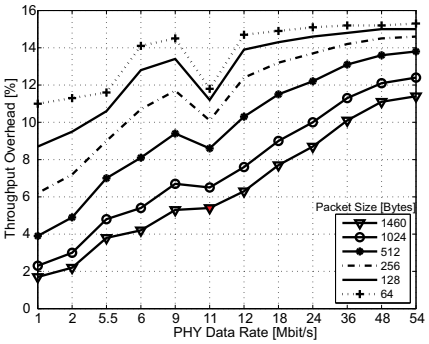

Fig. 2. Throughput overhead of the IEEE802.11 security frameworks in case of one hop link (theoretical).

Protocol Data Unit (MPDU) header by 16 Bytes. Bearing this and the time costs of the security operations in mind, the throughput overhead of the IEEE802.11 data transfer protection is given in equation (1).

$$Overhead_{Thr.} = \frac{(throughput_{Basic} - throughput_{Basic+Security}) \cdot 100}{throughput_{Basic}} \quad (1)$$

The parameters of equation (1) are calculated according to Table III with $MACOverhead_{Security}$ = MACOverhead + 16 Bytes. The results are depicted in Figure 2. The figure shows that the higher the PHY data rates and the smaller the frames are the higher is the overhead. This is justified by the lower transmission time of the frames in contrast to the constant time cost of the security functions (encryption of different packet sizes costs almost the same as it is run in hardware; the main encryption costs in Table I are more related to the supporting functions in software like loading the instructions from memory). Figure 2 shows that in case of IEEE802.11g, a throughput overhead of more than 10% might be induced, which typically gets higher in case of IEEE802.11n in HT mode and multiple spatial streams (MIMO). While this overhead is more related to one hop link, its impact on the overall performance of a network comprising several relay nodes between sender and destination is investigated in the next section.

As a matter of fact, this phase comprises a delay overhead. This overhead is however negligible in comparison to the time waited to access the medium as well as retransmission time costs and queuing effects that often arise.

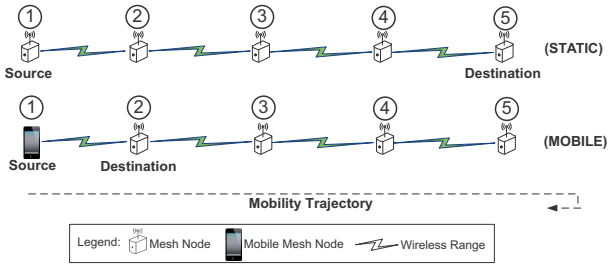

Fig. 3. Setup of the static and mobile chain mesh networks.

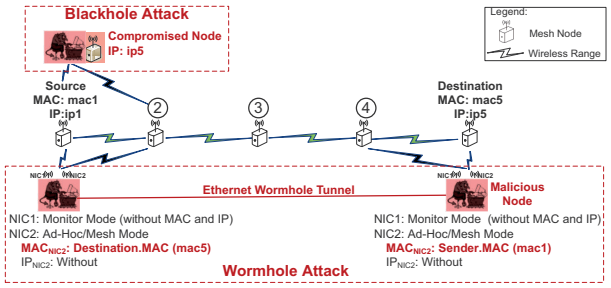

Fig. 4. Experimental testbed of the blackhole and wormhole attacks.

TABLE V
RELEVANT SIMULATION PARAMETERS.

Network and Traffic Models.

Parameter	Value
Carrier Sense Range [m]	341.8
Transmission Range [m]	267.1
Distance Between two Nodes [m]	175
Bitrate [Mbit/s]	11
BasicBitrate [Mbit/s]	1
MAC Layer	IEEE802.11g
Channel Model	Free-space
Simulation Time [s]	100
Velocity of Mobile Nodes [m/s]	10
Traffic Model	CBR-UDP
Packet Size [Bytes]	1460
Network Buffer Size [Packets]	100
Application Start, Stop Time [s]	0, 95
Number of Simulation Runs	10

Routing Protocol Configuration Parameters.

Protocol	Parameter	$Value_{static}$	$Value_{mobile}$
OGM/ HELLO-Interval	BATMAN/ OLSR	500ms	
TC-Interval	OLSR	1s	
RANN-Interval	HWMP	0s-reactive	
Neighbour-Hold-Time	HWMP, OLSR	12s	4s
Route-Hold-Time	ALL	15s	6s

III. PERFORMANCE AND SECURITY ANALYSIS

In this section, the IEEE802.11 security frameworks are first evaluated in the discrete event-based simulation environment OMNeT++ [29] and its INETMANET framework. Hereby, the static and mobile chain mesh networks illustrated in Figure 3 are considered. Simulation results are then validated in an experimental indoor testbed and differences between simulation and the practice are elaborated. Finally, the robustness of the security frameworks against the blackhole and wormhole attacks is investigated in the experimental indoor testbed scenario depicted in Figure 4.

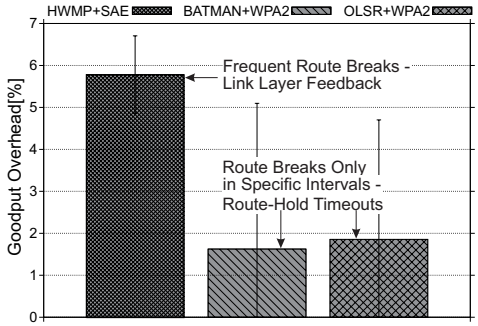

Fig. 5. Goodput overhead of the IEEE802.11 security frameworks in the static chain of 5 nodes (simulation).

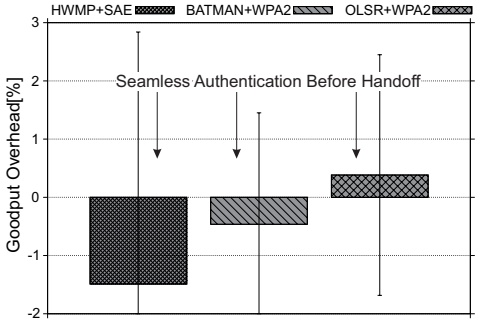

Fig. 6. Goodput overhead of the IEEE802.11 security frameworks in the mobile chain of 5 nodes - Underloaded network (simulation).

A. Simulation Configuration

The simulation configuration is depicted in Table V. The carrier sense range equals 341.8 m. According to the free space propagation model with a path loss exponent of 2.8, this is the maximum distance, in which a node equipped with a wireless interface having a receiver sensitivity of -91 dB can sense the signal in case the transmitting power is 20 dBm. The SNIR threshold is set to 4 dB, which means that in case the thermal noise is -101 dBm and the noise factor is 9 dB (NoiseLevel (mW) = $10^{\frac{(\text{thermal noise} + \text{noise factor})}{10}}$), the interference range of a link of length 175 m is approximately 277 m and the transmission range equals 267.1 m. That is, all the hidden nodes in the chain networks in Figure 3 lie within the interference range of the corresponding links (e.g., node3 interferes with node1). The PHY data rate is hereby 11 Mbit/s and the CBR-UDP application data rate is set to 1.85 Mbit/s. The latter is the highest data rate with HWMP achieving 100% packet delivery in case security is not activated.

B. Static Chain of 5 Nodes

This scenario is depicted in Figure 3 (top).

1) Simulation: The throughput overhead of the IEEE802.11 security frameworks and the collisions occurring during network setup, due to the simultaneous authentication of hidden nodes in the chain lead to the saturation of several nodes. Consequently, transmission errors occur. In case of HWMP and due to its link layer feedback mechanism, existing routes will be deleted due to the errors and HWMP will try to find the route again. In the meantime, incoming packets will be queued until the queue is filled up and queue-based packet drop occurs. As a result, we see in Figure 5 a relatively high goodput decrease of 6% in case of HWMP+SAE. In contrast to the frequent sporadic route breaks in case of HWMP, routes breaks occur in BATMAN and OLSR only in specific intervals, that correspond to either a route or a neighbour timeout. Therefore, the impact of the security overhead in this scenario is in general smaller than that of HWMP. Nevertheless, this impact is not negligible since typical audio and video codecs only tolerate up to 1% of packet error rates.

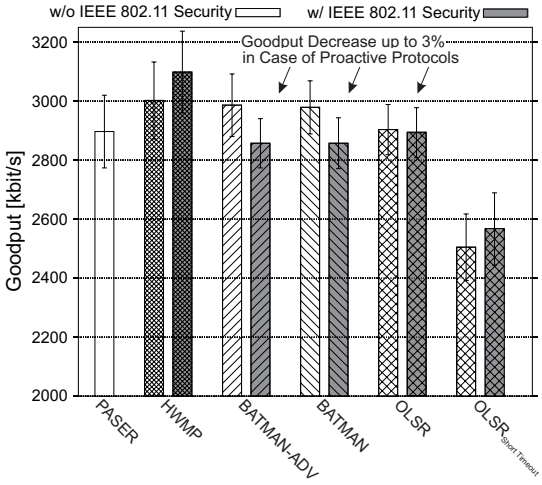

Fig. 7. Goodput evaluation in case of the IEEE802.11 security frameworks and PASER in the static chain of 5 nodes (experimental).

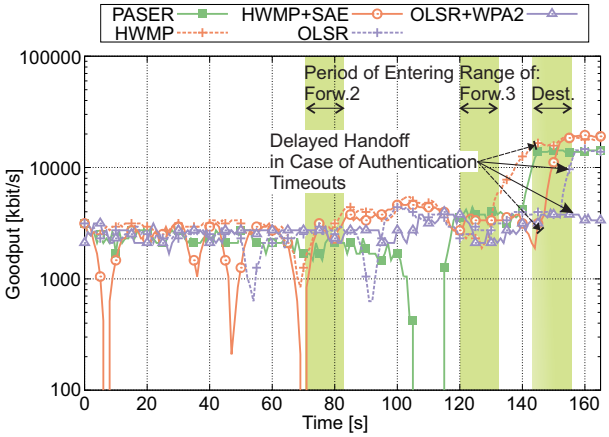

Fig. 8. Goodput evaluation in case of the IEEE802.11 security frameworks and PASER in the mobile chain of 5 nodes (experimental).

2) Experimental: The same mesh nodes as in [30] are used to setup the chain mesh network at two floors of our institute. Debian Wheezy with the 3.7 Linux kernel is installed on the nodes. For Wi-Fi Protected Access version 2 (WPA2) pre-shared key (the implementation of IEEE802.11i personal mode), hostapd-2012.09.10 is deployed and for SAE, the cozy-bit authsae-2013.06.05 implementation is used. The nodes are operating on channel 6 (IEEE802.11g). To reduce interferences from outside the network, the measurements are carried out at night. All measurements are performed using Iperf in TCP mode. Iperf in TCP mode delivers the available bandwidth in bit/s between sender and destination. The measurements have a duration of 100 seconds. Five repetitions for each measurement are performed.

Analogous to simulation, the goodput decreases up to 3% in case of proactive protocols if the security frameworks are running, as illustrated in Figure 7. However in contrast to

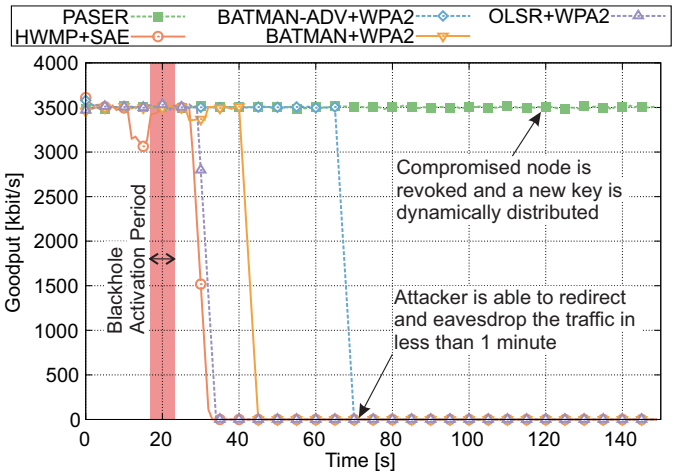

Fig. 9. Impact of the blackhole attack on the goodput in secured WLAN mesh networks (experimental).

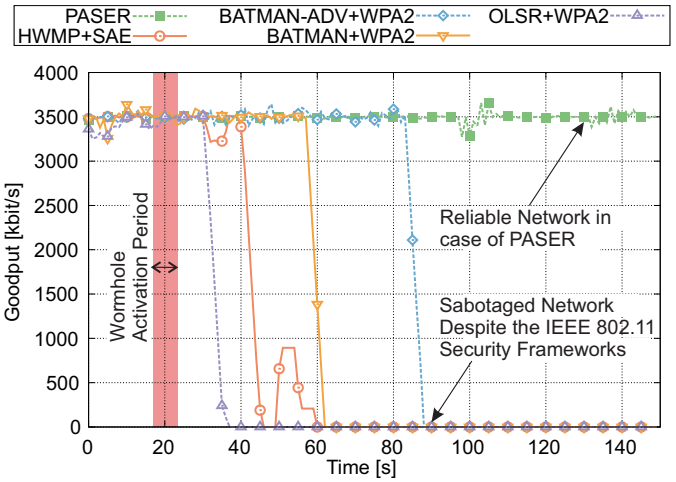

Fig. 10. Impact of the wormhole attack on the goodput in secured WLAN mesh networks (experimental).

simulation in case of HWMP (link layer feedback - highly sensitive to channel conditions), the security frameworks have relatively negligible impact on the performance. Hereby, sporadic transmission errors caused by hidden nodes, fading or external sources have a much higher impact on the network performance. To justify this observation, we reduced the timeouts in case of OLSR causing a route breaks if only six successive Hello messages of a neighbour could not be successfully received. As Figure 7 shows, in that case, the security overhead is no longer present.
Figure 7 also shows that the secure routing protocol PASER, which comprises, in contrast to its counterparts in related work, a key management scheme [31] and combines asymmetric and symmetric cryptosystems to exploit the advantages of both is competitive with the non-secure protocols in this scenario.

C. Mobile Chain of 5 Nodes

This scenario is depicted in Figure 3 (bottom).

1) Simulation: Figure 6 mainly sheds the light on two observations with respect to the mobile scenario. First, the authentication handshakes of the mobile node have no impact on the traffic flow. The mobile node is able to authenticate new nodes in its transmission range, upon receiving their beacons, before any routing protocol switches the route and use these nodes as next-hops. Second, since the traffic load of 1.85 Mbit/s is much lower than the network-throughput-optimal (number of forwarding hops ≤ 5), the impact of the overheads of the IEEE802.11 security frameworks in this scenario is negligible.

2) Experimental: Figure 8 shows that, as opposed to the controlled environment in simulation, the authentication phase of the security frameworks can delay an appropriate route switch causing a decrease in the goodput. A comparison of HWMP+SAE vs. HWMP as well as OLSR+WPA2 vs. OLSR in the period between 120 s and 140 s highlights this issue. It depicts that the protocols are able to faster shorten the route to the destination in case security is not activated. This is justified by the high number of authentication messages in case security is activated (8 times the number of neighbours), which could collide leading to the triggering of timeouts and thus delaying the route switch.

As in the static scenario, Figure 8 also shows that PASER has a comparable performance with the non-secure protocols in this scenario.

D. Static Chain of 5 Nodes under the Blackhole Attack

This attack has been implemented in the experimental testbed depicted in Figure 4 (top). Hereby, assuming the attacker has compromised a node/key, the attacker impersonates the destination (in general, the gateways in WMNs). Implementing the attack is quite straightforward as the attacker only needs to use the same IP address as the destination and the routing protocol will take care of the rest. In case of ISO-OSI layer 2 protocols such as HWMP or BATMAM-ADV, ARP spoofing is also required. This can be carried out with a simple *ping* command. Unfortunately, not only direct neighbours are affected by this attack but also other nodes located outside the range of the attacker because the routing protocol running will disseminate the fake identity of the attacker throughout the whole network. As a result, the attacker can redirect the traffic and sabotage the network. As Figure 9 shows, in less than one minute after starting the attack, all non-secure protocols combined with the IEEE802.11 security frameworks get caught in the attacker's trap. That is, the IEEE802.11 security frameworks are not able to mitigate the attack. This means that in case this attack is carried out, the network operator has to collect all the nodes, reconfigure them, and setup the network again. In contrast, in case the secure routing protocol PASER is running and due to its dynamic key management scheme and its security features, the compromised node is revoked and the network key is dynamically refreshed. Therefore, the performance of the network is not affected by this attack in case PASER is used, as depicted in Figure 9.

E. Static Chain of 5 Nodes under the Wormhole Attack

To carry out this attack, two malicious nodes directly connected with each other (using, e.g., LAN or directional antennas, etc.) are placed at the incident scene, as depicted in Figure 4 (bottom). These nodes transparently forward routing messages faster than legitimate nodes from one area of the network to another, i.e., from source to destination. This causes affected nodes located in different areas to believe that they are neighbours and start sending their messages via the wormhole tunnel instead of using legitimate relay nodes. The attacker

can then drop all data packets causing a sabotage of the network. In contrast to the blackhole attacker, the wormhole attacker do not require network access. To implement this attack, the attacker just needs two interfaces per node: The first is set to monitor mode to eavesdrop all the frames in the proximity, regardless of their destination, and the second is set in ad-hoc/mesh mode to automatically reply with an ACK frame to any unicast packet sent to the victim nodes. In this way, the legitimate nodes will never detect that the network is sabotaged. To sabotage the network, the attacker forwards the routing messages to manipulate the routing topology and the attacker discards the data packets. For the case when the IEEE802.11 security frameworks are employed, routing messages and UDP/TCP data packets are both encrypted in data frames, thus, the attacker cannot decide based on the content whether to forward the frame or not. However, as routing messages are typically smaller than 500 Bytes while videos and pictures (data) are typically larger than 1300 Bytes, the attacker can decide based on the size of the frame whether to forward it (more intelligent attackers could designate the frames content based on their frequency). Figure 10 shows that non-secure routing protocols in combination with the IEEE802.11 standard security frameworks are prone to the wormhole attack. How fast the wormhole is established depends on the protocol design and metrics. In case of OLSR, since the route quality is the average of the qualities of all one hop links that build the route (ETX metric), the attack occurs very fast. In case of BATMAN (layer 3) and BATMAN-ADV (layer 2), the route is selected based on the number of OGMs received within a sliding interval. Consequently, it takes a slightly longer time to use the wormhole tunnel than in case of OLSR. In case of HWMP, the success of the attack is very fast as HWMP practically sends a route request every 4 seconds to refresh active routes. Only PASER shows to be robust against the wormhole attack, due its geographical leash mechanisms and its security features [32].

IV. Conclusion

In this paper, we analyze the security frameworks of the IEEE802.11s and IEEE802.11i standards with respect to performance and security in WMNs. We show that these frameworks have in general a slight overhead in small WMNs. Nevertheless, the high number of authentication messages and the throughput overhead of these frameworks might lead to a considerable goodput degradation. From the security perspective, we experimentally show that the IEEE802.11 security frameworks are not able to mitigate the blackhole and wormhole attacks and, thus, they can not be used to establish reliable networks. We conclude that using these security frameworks in the backbone of WMNs is not as appropriate as their conventional use to secure the communication between mesh access points and clients. To this end, an efficient secure routing protocol combined with a dynamic key management scheme are inevitable to establish a reliable network, as we experimentally show using PASER as an example. For the protection of the data transfer in the backbone, end-to-end security solutions such as IPsec could be used. As a result, no throughput overhead caused by unnecessary per hop encryption and decryption is encountered as in the case of the IEEE802.11 security frameworks.

Acknowledgment

Our work has been conducted within the AIRBEAM project, which is funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261769.

References

[1] A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance evaluation of process-oriented wireless relay deployment in emergency scenarios," in *IEEE ISCC*, 2012.
[2] N. Goddemeier, K. Daniel, and C. Wietfeld, "Role-based connectivity management with realistic air-to-ground channels for cooperative uavs," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 5, 2012.
[3] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Elsevier Ad Hoc Networks*, vol. 2, no. 1, 2004.
[4] P. Avakul *et al.*, "Mesh router selection to maximize system throughput in dense wireless mesh networks," in *IEEE HPSR*, 2013.
[5] A. Abdulla *et al.*, "Hymn: A novel hybrid multi-hop routing algorithm to improve the longevity of wsns," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, 2012.
[6] H. Yih-Chun and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security and Privacy*, vol. 2, no. 3, 2004.
[7] L. Abusalah, A. Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad hoc Routing Protocols," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, 2008.
[8] (2013, Sep.) Wireless Battle Mesh. [Online]. Available: http://battlemesh.org/
[9] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11, 2012.
[10] (2013, Sep.) Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.). Freifunk Community. [Online]. Available: http://www.open-mesh.org/
[11] T. Clausen and P. Jacquet, "Optimized Link State Routing (OLSR) Protocol," RFC 3626, 2003.
[12] B. Kannhavong *et al.*, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 5, 2007.
[13] K. Sanzgiri *et al.*, "Authenticated Routing for Ad hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, 2005.
[14] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *ACM WiSe*, 2002.
[15] F. Hong, L. Hong, and C. Fu, "Secure olsr," in *AINA*, 2005.
[16] M. Sbeiti, J. Pojda, and C. Wietfeld, "Performance Evaluation of PASER - an Efficient Secure Route Discovery Approach for Wireless Mesh Networks," in *IEEE PIMRC*, 2012.
[17] J. Ben-Othman and Y. Saavedra Benitez, "On securing hwmp using ibc," in *IEEE ICC*, 2011.
[18] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Communications*, vol. 11, no. 1, 2004.
[19] "A comparison between traditional public key infrastructures and identity-based cryptography," *Information Security Technical Report*, vol. 8, no. 3, 2003.
[20] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," *ACM Journal on Wireless Networks*, vol. 11, no. 1-2, 2005.
[21] Y. Hu, D. Johnson, and A. Perrig, "Secure efficient distance vector routing in mobile wireless ad hoc networks," in *IEEE WMCSA*, 2002.
[22] W. Galuba *et al.*, "Castor: Scalable Secure Routing for Ad Hoc Networks," in *IEEE INFOCOM*, 2010.
[23] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Std 802.11, 2004.
[24] G. Lukas and C. Fackroth, "Wmnsec: security for wireless mesh networks," in *IWCMC*, 2009.
[25] A. Egners, H. Fabelje, and U. Meyer, "Fsasd: A framework for establishing security associations for sequentially deployed wmn," in *IEEE WoWMoM*, 2012.
[26] Y. Zhang, J. Zheng, and H. Hu, *Security in wireless mesh networks*. Auerbach Publications, 2008.
[27] O. Cheikhrouhou, M. Laurent-Maknavicius, and H. Chaouchi, "Security architecture in a multi-hop mesh network," in *SAR*, 2006.
[28] T. Bird, "Measuring function duration with ftrace," in *Linux Symposium*, 2009.
[29] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *SIMUTools*, 2008.
[30] J. Pojda *et al.*, "Performance analysis of mesh routing protocols for uav swarming applications," in *ISWCS*, 2011.
[31] (2013, Sep.) Postion Aware Secure and Efficient Mesh Routing Protocol (PASER). Communication Networks Institute, TU Dortmund, Germany. [Online]. Available: http://www.paser.info/
[32] M. Sbeiti, J. Hinker, and C. Wietfeld, "VLX: A Novel Virtual Localization Extension for Geographical Leash-based Secure Routing in Indoor Wireless Mesh Scenarios," in *IEEE WiMob*, 2012.