Protecting IEEE 802.11s Wireless Mesh Networks Against Insider Attacks

Andreas Reinhardt, Daniel Seither, Andre König, Ralf Steinmetz
Multimedia Communications Lab
Technische Universität Darmstadt
{andreas.reinhardt, dseither, akoenig, ralf.steinmetz}@kom.tu-darmstadt.de

Matthias Hollick
Secure Mobile Networking Lab
Technische Universität Darmstadt
matthias.hollick@seemoo.tu-darmstadt.de

***Abstract*—IEEE 802.11s is an emerging standard for wireless mesh networks. Networks based on IEEE 802.11s directly benefit from existing security mechanisms in IEEE 802.11. This limits the attack surface of IEEE 802.11s significantly for adversaries that cannot authenticate with the network. Mesh networks are, however, often conceived for community network scenarios, which are inherently more open than managed infrastructure networks. This openness entails an increased risk of insider attacks, i.e., attacks by compromised stations that *can* authenticate with the network. Currently, IEEE 802.11s is lacking adequate protection against such insider attacks. In this paper, we hence derive an attack model for insider attacks and present two insider attack strategies to which IEEE 802.11s networks are prone, namely impairing the network performance and preventing communication between a pair of nodes. We design countermeasures that allow to defend the wireless network against both types of attacks. Our implementations only incur marginal computational and memory overheads, while the network security is measurably strengthened.**

I. Introduction

In contrast to the IEEE 802.11 infrastructure and ad hoc networking modes [3], the IEEE 802.11s [4] standard introduces the notion of wireless mesh networks. Practical application areas for wireless mesh networks include the provision of network coverage in rural areas, extending the edge of existing networks without deploying dedicated infrastructure, or establishing community networks. Because IEEE 802.11s has been designed to leverage existing hardware and firmware of IEEE 802.11 devices, it can potentially be deployed to the billions of WiFi-enabled devices globally in use to date[1].

In order to secure the wireless mesh communications, IEEE 802.11s offers a number of security mechanisms derived from the original IEEE 802.11i standard, which have been merged into IEEE 802.11-2007 [3]. These mechanisms protect against certain attack vectors, commonly in the form of *outsider attacks*, in which the attacker does not have access to the network's authentication credentials. An increased risk of *insider attacks* is given when moving towards open network models like IEEE 802.11s, in which each individual station is part of the access infrastructure. Dedicated security mechanisms for wireless LANs in which the attacker can successfully authenticate with the network thus remain to be found.

[1]A market forecast by IHS iSuppli (http://www.isuppli.com) published in 2/2011 estimate the number of annually shipped Wi-Fi chipsets to surpass 1 billion units *per year* in 2012.

We target the analysis and mitigation of insider attacks in this paper and conduct a detailed analysis of possible insider attacks by means of the attack tree methodology (Sec. II). Furthermore, we design solutions to mitigate the determined threats and shortcomings of the IEEE 802.11s standard (Sec. III). We discuss related work on IEEE 802.11s security in Sec. IV, and conclude this paper in Sec. V.

II. Attacks on IEEE 802.11s

After briefly revisiting the terminology used in this paper, we present a systematic model of potential attacks on the security of IEEE 802.11s. Our primary goal is to find the attack vectors that are most attractive to malicious insiders. The identification of these attack vectors represents the basis on which we later design security mechanisms that render attacks less attractive by significantly increasing their cost.

A. Terminology and Introduction to IEEE 802.11s

The basic entities are introduced in this section according to the IEEE 802.11-2007 [3] and IEEE 802.11s [4] standards. A *station* (STA), defined as any device that has physical access to the wireless medium and implements the IEEE 802.11 standard, is the basic entity of a wireless LAN. For their addressing, STAs use 48-bit hardware (MAC) addresses. A set of wirelessly connected STAs forms a *Basic Service Set* (BSS). The amendment *'s'* adds the *Mesh BSS* (MBSS) to the wireless LAN standard. An MBSS enables multi-hop communication between mesh STAs on the MAC layer, which is transparent to higher layers of the networking stack. The IEEE 802.11s standard also defines a routing protocol, the *Hybrid Wireless Mesh Protocol* (HWMP) [4].

Although HWMP is based on the AODV protocol [8], MBSS communication is realized on the MAC layer, and as such, HWMP relies on MAC addresses for routing. Besides adopting the purely reactive character of AODV, HWMP also offers optional proactive elements to establish tree-like topologies, making it a *hybrid* routing protocol. As a result of these major changes to the routing protocol's behavior, the names of routing control messages also differ between AODV and HWMP. This results from the fact that HWMP operates on layer 2 of the ISO-OSI networking stack, and thus relies on *paths* rather than using *routes*. The messages are thus termed Path Request (PREQ), Path Reply (PREP), and

978-1-4673-1564-7/12/$31.00 ©2012 IEEE

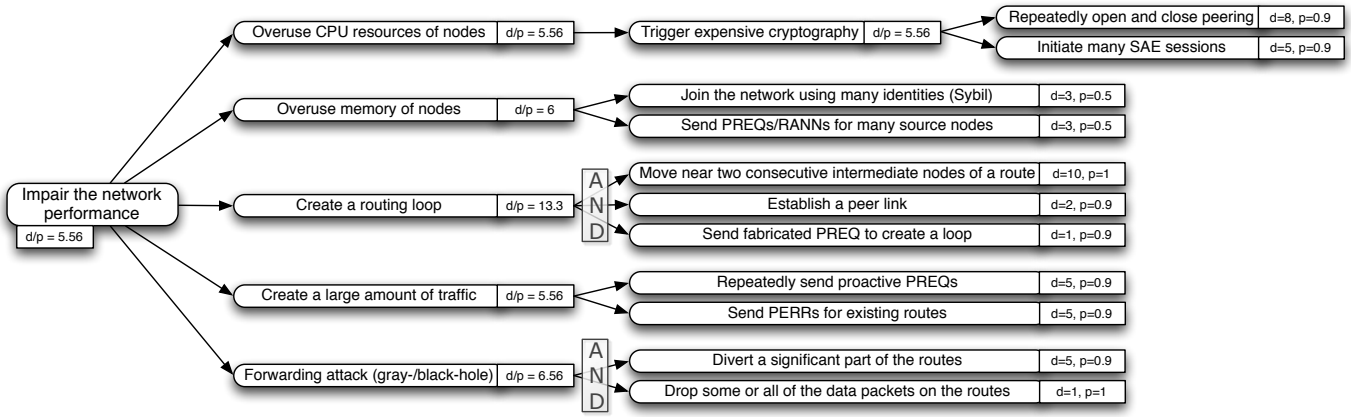

Fig. 1. Attack tree for attacks that impair the network performance

Path Error (PERR). Moreover, the hop-count routing metric of AODV is replaced by an extensible path selection framework, which allows for advanced metrics. With regard to its security, IEEE 802.11s introduces the *Simultaneous Authentication of Equals* (SAE) protocol [2]. It establishes a cryptographically strong secret based on the mutual knowledge of a simple password, thus representing a viable alternative when central authentication servers are unavailable.

B. Scope and Methodology

First and foremost, this paper focuses on attacks from users authenticated to the network, i.e., insiders. Furthermore, we assume that the network is configured using the state-of-the-art security services of IEEE 802.11, e.g., WPA2. We confine our analysis to attacks on the MAC sublayer of the wireless LAN and do not consider the modification of higher-layer data as a successful attack. Attacks must have an impact on more than just the direct neighbors of the attacker, or they must have other significant benefits over simple jamming on the physical layer. Finally, all Mesh STAs strictly adhere to the standards, i.e., we do not consider vulnerabilities that are introduced by the implementer of the networking stack.

To model attacks on IEEE 802.11s, we use the attack tree method described by Schneier in [10]. The attacker's main goal is used as the root of the tree. Different approaches to reach this goal are represented by child nodes (subgoals) of the tree root. This subdivision is carried out recursively until basic actions are reached that form the leaves of the tree and are specific enough to be implemented. We assume a disjunction of the children unless the connection is annotated with *AND*, in which case the attack described in the tree node is only considered successful if all of its children are successful. Attack trees cannot only be used to show the different ways to achieve an attacker's goal but also to evaluate the difficulty of such attacks and their probability to succeed. Specifically, we estimate the difficulty d, ranging from 1 (very simple task) to 100 (very complex task), and the success probability p, which ranges between 0 and 1 and describes the probability that an action has the desired outcome (defined in its parent node) if carried out correctly.

C. Attacker's Goals

As we confine our analysis to the MAC sublayer and only focus on attacks that have an impact beyond the one hop neighborhood, the routing process of IEEE 802.11s is the sole target with notable attack surface. We have identified two primary attacker goals, which are described as follows.

a) Impairing the network performance: Network performance can be impaired by attacks on the network's resources (e.g. CPU and memory usage of the STAs or their available airtime) and/or on the routing process itself. The complete attack tree devised for attacks on the network performance is visualized in Fig. 1. Each node in the attack tree is annotated by its difficulty and success probability or their quotient. First of all, the repeated connection and disconnection between neighboring nodes always requires the execution of costly cryptographic operations. Besides overusing CPU resources, the excessive demand for STA memory can also be used for attacking a node. An attacker can repeatedly create a new identity (i.e., a new MAC address), and then create security associations/peerings with one or multiple neighbors. While he can purge all data when switching to a new identity, its neighbors accumulate large amounts of stale state information.

The creation of routing loops has a high d/p ranking in our attack tree and is thus considered harder to achieve. Its most complicated component is to physically move near two intermediate nodes on a route. Once in this position, the attacker can transmit a specially crafted PREQ in order to create a routing loop which keeps the involved STAs busy by forwarding the same data frames back and forth until their TTL field expires [1]. An attacker can also repeatedly send PREQs to cause a high amount of traffic in the whole network [7]. Because the frame is flooded to all STAs, each of them replies with a PREP if the frame is a proactive PREQ and replies were requested. As a result, this leads to a Distributed Denial of Service attack on the neighbor nodes. Finally, selective forwarding attacks represent the fifth class of attacks on the network performance. In order for this attack to be successful, routes must firstly be diverted to involve the malicious node. Subsequently, the attacker simply drops some or all of the forwarded data.

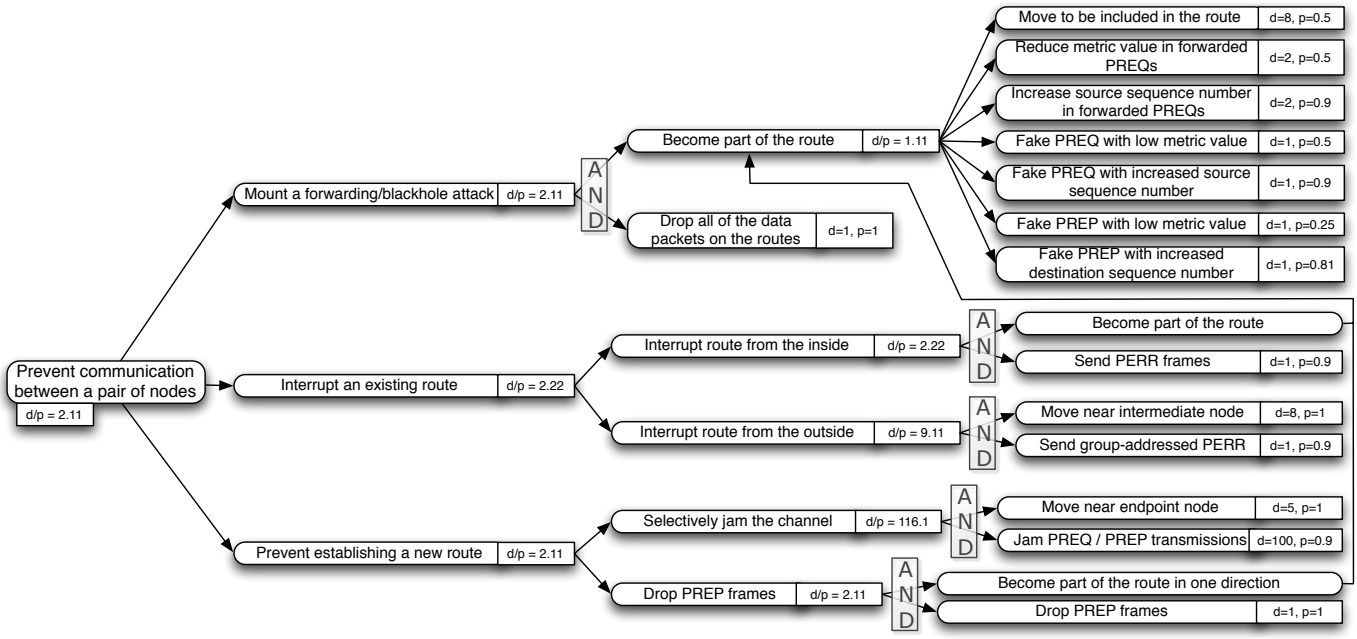

Fig. 2. Attack tree for the goal of preventing communication between a pair of nodes

b) Prevent communication between a pair of nodes: The ways for achieving the goal of preventing communication between a pair of nodes are modeled in Fig. 2, and selected means are discussed as follows. Becoming part of a route is essential for numerous attacks. If the metric value in forwarded PREQs for the given route is reduced by the attacker, the probability rises that he will be included in the resulting route. Similarly, when the source sequence number is increased in forwarded PREQs, the resulting route seems fresher than any real route and is thus preferred over others. The HWMP protocol relies on PERR frames in order to invalidate routes. Besides their intentional transmission while the attacker is included in the route, PERR frames can also be injected into an existing route between a given pair of nodes. The difference is that the attacker needs to use the address of the intermediate node from the previous step as the sender address and to encrypt the frame using the neighbor's mesh group temporal key, so that the PERR is accepted by other STAs in the route.

Routes can also be interrupted from the outside, either by sending group-addressed PERR frames, or by jamming the channel when transmission of relevant PREQ or PREP is in progress. An attacker listens to the channel and starts jamming as soon as he detects an ongoing transmission of a frame that contains a PREQ or PREP for the given pair of nodes.

III. Design of Security Extensions

Having identified the vulnerabilities of IEEE 802.11s, we show that the attack surface of an MBSS can be significantly reduced by investing a certain amount of network resources into extended proactive security.

A. End-to-end Data Authentication

The first proposed security extension is end-to-end data authentication, which is achieved by appending a digital signature of the immutable parts of the routing element to each frame. In order for this end-to-end data authentication to work properly, PREP generation by intermediate nodes must be disabled, as intermediate STAs cannot create signatures for the destination STA of the route. Similarly, PERR frames are signed at each hop, but STAs only forward information for which the last transmitter of the PERR is the next hop, as only these routes have been broken. Finally, to ensure that mutable fields that have been changed in value en route do not impair the operation of the signature, they must be excluded from the set of data which is signed. An extension to also protect these mutable fields is presented as follows.

B. Protection of Mutable Data

In Route Announcements (RANNs), PREQs and PREPs, three fields, namely the Hop Count, Time to Live (TTL), and Metric elements are mutable and thus cannot be protected by aforementioned approach. We focus on the protection of the metric elements using hash chains, because the hop count field is neither used to make routing decisions in HWMP, nor could we come up with any significant attacks that exploit unprotected TTL values. Due to the large increments and the large total size of metric values, however, their protection is complex. The Airtime Link Metric uses 4 bytes which would lead to a hash chain length of 2^{32}, or more than 4 billion steps. This motivated us to introduce a function which maps the metric value to a smaller range of numbers, described as follows. If we assume a link operating at 54MBit/s in the absence of transmission errors, we get the lower bound of 153μs. As $log_2(153)>7$, the lower 7 bits of the metric value do not carry relevant information and can be discarded. Similarly, for a link operating at the minimum data rate of 1MBit/s and with an error rate of 75%, we get an upper bound of

32772μs. Its $log_2(32772) \approx 15$ shows that bits 16 to 32 are unnecessary. When looking at these bounds, we can see that the dynamic range of a single hop's metric is around 15-7=8 bits. Considering the addition of hop-by-hop values to the end-to-end metric, $log_2(\#hops)$ must be added to this value.

C. Hop-by-hop Data Authentication for Broad- and Multicasts

Our third improvement to the HWMP protocol addresses the fact that broadcast frames are not authenticated in an end-to-end manner. In order to send a PERR to its neighbors, a STA uses the pairwise keys negotiated with its neighbors to calculate a hash-based message authentication code (HMAC) for each of the neighbors. This list of HMACs is then appended to the frame, so that each neighbor will find one HMAC that it can verify. We propose that HMACs are calculated for HWMP frames if they contain one or multiple PERRs, and thereby protect their contents. The HMACs are stored in a new element at the end of the frame as seen in Fig. 3. The indices #1 to #n denote the n neighboring peers.

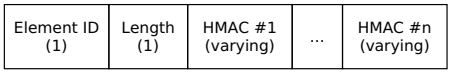

Fig. 3. Structure of the hop-by-hop data authentication element

The receiver calculates the HMAC of the data using the pairwise key shared with the sender and compares the resulting value to each transmitted HMAC. Each match indicates that the frame was transmitted by the corresponding peer and the index within the list of HMACs is stored. When the receiver receives further messages from the same peer, it first uses the HMAC at the stored index for comparison. The communication overhead grows linearly with the number of peers, as does the time for the first lookup from the list of HMACs at the receiver side. However, as the number of peers of a single node is tightly bounded and another peer only adds the length of one HMAC to the message, this simple solution is feasible.

IV. Related Work

With regard to the contributions of this paper and the focus on the routing protocol (cf. Sec. II-C), we confine our presentation of related work to contributions in this field. AODV [8] itself does not specify any security mechanisms and thus is susceptible for a great range of attacks. Ning and Sun [7] give a systematic overview of AODV's vulnerabilities, which we have used as a basis for our security analysis of IEEE 802.11s. Secure AODV [11] assumes that each node is assigned a certificate and knows the corresponding private key, which is used to perform end-to-end authentication of routing packets, and relies on hash chains to protect mutable data. The ARAN protocol [9] is similar to AODV, but introduces authentication using digital certificates. Route discovery packets are signed in both end-to-end and hop-by-hop fashion, which increases the security, but incurs a high computational overhead. For its use in IEEE 802.11s networks, Secure HWMP [5] prevents PREQ flooding, route disruption, and route diversion attacks. Since all the mechanisms only use hop-by-hop data authentication, each intermediate node can modify or forge frames without any restriction. Trust-based HWMP [6] does not directly prevent attacks but describes a mechanism to let STAs quantify trust in their peers, using packet loss as a metric of trust. If the trust value of a STA as perceived by its neighbors falls below a certain value, the STA is no longer used for routing.

V. Conclusion

The IEEE 802.11s standard can be used to create a mesh network that offers a high level of security against outside attackers. However, as soon as an adversary is able to enter the network by capturing a STA or by gaining valid authentication credentials, almost all security mechanisms become ineffective. In this paper, we have presented the first steps towards better security in the presence of inside attackers by systematically analyzing the attack vectors that an adversary can use and identifying the ones that are most easily exploited. We have designed three security extensions for IEEE 802.11s, which provide proactive security mechanisms against malicious insiders. Even in case of sophisticated attacks that cannot be prevented by our security extensions, they enable reliable identification of malicious mesh STAs, thus laying the groundwork for reactive security mechanisms, such as intrusion detection systems.

Acknowledgment

This work was supported by LOEWE CASED (www.cased.de).

References

[1] C. Gottron, P. Larbig, A. König, M. Hollick, and R. Steinmetz, "The Rise and Fall of the AODV Protocol: A Testbed Study on Practical Routing Attacks," in *Proceedings of the 35th IEEE Conference on Local Computer Networks (LCN)*, 2010.

[2] D. Harkins, "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks," in *Proceedings of the International Conference on Sensor Technologies and Applications (SENSORCOMM)*, 2008.

[3] IEEE 802.11-2007, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE Press, 2007.

[4] IEEE 802.11s-2011, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 10: Mesh Networking*. IEEE Press, 2011.

[5] M. S. Islam, Y. J. Yoon, M. A. Hamid, and C. S. Hong, "A Secure Hybrid Wireless Mesh Protocol for 802.11s Mesh Network," in *Proceedings of the International Conference on Computational Science and Its Applications (ICCSA)*, 2008.

[6] R. Matam and S. Tripathy, "THWMP: Trust-Based Secure Routing for Wireless Mesh Networks," in *Proceedings of the International Conference on Communication, Computing & Security (ICCCS)*, 2011.

[7] P. Ning and K. Sun, "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols," *Ad Hoc Networks*, vol. 3, no. 6, 2005.

[8] C. Perkins, E. Belding-Royer, and S. Das, *Ad hoc On-Demand Distance Vector Routing*, RFC 3561, Internet Engineering Task Force Std., 2003.

[9] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, 2005.

[10] B. Schneier, "Attack Trees – Modeling security threats," *Dr. Dobb's Journal*, 1999. [Online]. Available: http://www.schneier.com/paper-attacktrees-ddj-ft.html

[11] M. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," in *Proceedings of the 1st ACM Workshop on Wireless Security (WiSe)*, 2002.