Differentiated Security in Wireless Mesh Networks*

Thomas Gamer
gamer@tm.uka.de

Lars Völker
voelker@tm.uka.de

Martina Zitterbart
zit@tm.uka.de

Institute of Telematics, University of Karlsruhe, Germany

ABSTRACT

The upcoming IEEE 802.11s standard enables easy establishment and maintenance of wireless mesh networks in residential and enterprise scenarios. They, however, need some special attention with respect to security. Due to multi-hop communication and routing on layer 2 in mesh networks, attacks on the routing, selective forwarding, and eavesdropping on confidential data become relatively easy. To avoid such attacks, we introduce differentiated security which is based on protection levels associated with nodes in the network. Participation in the MAC layer routing is facilitated according to the respective protection level of a node. Using additional cryptographic protection our approach can also avoid unintentional disclosure of confidential data.

Categories and Subject Descriptors: C.2.0 [Computer-Communication Networks]: General—*Security and protection*; C.2.1 [Computer-Communication Networks]: Network Architecture and Design—*Wireless communication*

General Terms: Security

Keywords: Security, Routing, Wireless Mesh Networks

1. INTRODUCTION

Wireless mesh networks currently are standardized by the IEEE 802.11s [2] Task Group. In such easy to establish wireless networks, mobile wireless nodes and infrastructure devices are used for routing. This provides higher flexibility and network coverage and decreases administration and infrastructure overhead. Mesh networks primarily are suitable for residential and enterprise scenarios.

But there also are challenges because physical access on the transmission medium cannot be restricted in wireless networks in general. Thus, attacks like eavesdropping, changing frame content, and taking part in the communication are possible if no appropriate security mechanisms are used.

In contrast to the single-hop communication used in IEEE 802.11 [1] wireless networks, mesh networks apply routing mechanisms on layer 2 based on MAC addresses in order to achieve multi-hop communication. This means that each node taking part in the mesh network has to forward frames according to a specific MAC layer routing protocol, e. g. Hybrid Wireless Mesh Protocol (HWMP) [2]. In the following we are speaking of *path selection* instead of MAC layer routing in order to make the difference to layer 3 routing more obvious. Due to the path selection and multi-hop communication on MAC layer, new attacks like selective forwarding, maliciously influencing the routing protocol, or eavesdropping on forwarded data and path selection messages become relatively easy. Attackers in these cases are internal malicious nodes that legitimately take part in the mesh network.

Our main contributions to avoid attacks by internal and external attackers in mesh networks are

- *Introduction of a differentiation of nodes and traffic.*
- *Introduction of appropriate cryptographic protection.*

The basic concept of differentiated security in mesh networks and related work will be presented in the following Section. Section 2.1 gives a detailed example.

2. BASIC CONCEPT

The concept of differentiated security in mesh networks provides a separation of data as well as routing traffic. This means, network data traffic is divided into different *traffic classes* dependent on the respective protection the traffic needs. In addition, nodes participating in the mesh network are assigned a certain *protection level*. This protection level represents the trust in the respective node, i. e. should the node be able to forward certain traffic and read the frame contents. This, in turn, means that the nodes are able to participate in the path selection protocol according to their respective protection level. Thus, path selection is influenced in a way that frames are forwarded to *trusted* nodes only. This reduces possibilities of attacks for internal malicious nodes significantly. In order to secure such a separation of traffic, additional cryptographic protection is necessary.

One of the approaches very similar to our work are Virtual LANs (VLANs) [3] for Ethernet networks. VLANs allow for transport of different virtual networks over a single network by tagging the frames. The difference to our work is that we are using a wireless network instead of wired Ethernet. Attackers in wired networks have often only access to a single port or link, and do commonly not forward frames for other nodes. In mesh networks nodes have to forward frames and attackers may easily eavesdrop on all links at once.

Another easy solution for separation of nodes and traffic would be a partitioning into different mesh networks. This, however, results in bad network coverage and unreachable nodes get more likely within each network. Furthermore, multiple radios would be necessary if nodes want to participate in multiple networks, e. g. since various communications should be protected differently. Therefore, in our solution

*We gratefully acknowledge that this work was funded by Siemens Enterprise Communications GmbH & Co. KG

Q2SWinet'08, October 27–28, 2008, Vancouver, BC, Canada.
ACM 978-1-60558-237-5/08/10.

nodes can be assigned multiple protection levels at the same time and thus, a single mesh network is sufficient.

Some existing solutions, e. g. [5, 6], try to avoid attacks of internal nodes by rewarding correct behavior using virtual currency or by using a reputation-based approach. Trust-based routing mechanisms in ad-hoc networks, e. g. [6], try to avoid forwarding frames to malicious nodes by observing, rating, and distributing the behavior of neighbor nodes continuously. In case of mesh networks, our solution takes advantage of the fact that some knowledge about the participating nodes exists in advance and thus, assignment of protection levels can be done statically. In addition, enabling a node to take part in multiple protection levels is less complex based on meta knowledge than with dynamically calculated trust levels.

Having explained how and why we apply a differentiation of nodes the way we do, we will present now how to achieve cryptographic protection for this concept. The IEEE 802.11 standard defines Robust Secure Network (RSN) for protection of the network from external attackers. Authentication and key distribution in large enterprise networks is commonly achieved using an authentication server. In residential and small enterprise scenarios, nodes are mostly authenticated based on preshared keys. IEEE 802.11s is based on RSN and proposes an extended key hierarchy with an additional indirection level. Data traffic is protected hop-by-hop by pairwise keys in both cases. Routing and management frames, however, are neither protected by RSN nor by IEEE 802.11s security mechanisms.

We propose usage of multiple group keys—one per protection level—based on RSN for protection of differentiated security. Group keys have some advantages over pairwise peer keys as used in IEEE 802.11s: Data and path selection traffic can be easily secured by a single key, a lower number of keys is used and each node must communicate with the key distributor just once before being able to take part in path selection and communication with other nodes.

2.1 Detailed example: Small enterprise mesh

Figure 1 shows an exemplary small enterprise scenario with 8 mesh nodes and 1 authentication server (AS). Node A is a Mesh Portal Point (MPP). This node provides a connection to the authentication server and to other networks, e. g. the Internet. The other nodes are called Mesh Points (MP). All mesh nodes participate in the path selection protocol used in this particular WLAN mesh. Legacy IEEE 802.11 nodes that can be transparently integrated into mesh networks are not considered in this paper. Two different protection levels are defined. In the following, the value representing a specific protection level is called *Type of Protection (ToP)*. The two protection levels in our small example are represented by the ToPs *Visitor* and *Employee*.

Visitor nodes are only allowed temporarily to participate in the mesh network and do not belong to the enterprise in most cases. Nevertheless, these nodes can also be mesh-capable and take part in the network as mesh nodes. Thus, visitor mesh nodes get a different ToP than employee nodes. Since ordering of ToPs would restrict flexibility of ToP mapping too much and partitioning into protection levels should be avoided our concept allows for assignment of multiple independent ToPs to a node. This enables such nodes to forward traffic of other ToPs. *Employee nodes*, in our example, should be trusted more than visitor nodes and therefore, some of the employee nodes additionally get the ToP *Visitor* assigned. This ensures that these nodes—nodes A, C, D, and E in our example—are able to forward all traffic of this mesh network. Nodes that e. g. aim at low energy consumption, like node G, may reduce radio usage by only forwarding frames of their own ToP. With our solution partitioning and unreachable nodes due to unfavorable number of ToPs or disadvantageous ToP assignment to participating nodes are not impossible but less likely than in separated mesh networks.

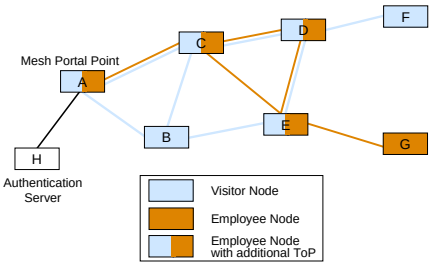

Figure 1: Exemplary small enterprise scenario

After initial authentication each node gets its ToPs and the associated group keys from the authentication server. Transmission of these keys is secured by the Pairwise Master Key (PMK) between authenticating node and authentication server, which is derived during authentication. Afterwards, the node is able to take part in the path selection protocol. Path selection messages are protected by the group keys. Consequently, this results in multi-path routing with one forwarding table per associated ToP on each node. This prevents malicious nodes of other ToPs from influencing path selection since they do not posses the necessary ToP group key the path selection messages are protected with. Furthermore, data traffic is protected by ToP group keys, too. Therefore, a ToP must be assigned to each frame. Subsequently, frames are forwarded only to trusted nodes on their way through the mesh network, i. e. according to the forwarding table of the appropriate ToP. Furthermore, it is ensured that—due to the cryptographic protection—only nodes that possess the correct ToP group key are able to read the frame content.

Differentiated security cannot keep internal malicious nodes within the protection level from successfully carrying out attacks like selective forwarding; however, differentiated security allows us to reduce the number of possible attackers to a minimum and keeps internal nodes outside the protection level from attacking successfully.

3. REFERENCES

[1] IEEE Computer Society. IEEE Standard for Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.

[2] IEEE Computer Society. IEEE P802.11s/D2.0 – Draft STANDARD for Local and Metropolitan Area Networks – Specific Requirements – Amendment to Part 11: Mesh Networking, March 2008.

[3] IEEE Computer Society. IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks, May 2003.

[4] D. Kraft and G. Schafer. Distributed access control for consumer operated mobile ad-hoc networks. In *Proc. of First IEEE CCNC*, pages 35–40, 5–8 Jan. 2004.

[5] B. Lamparter, K. Paul, and D. Westhoff. Charging support for ad hoc stub networks. *Computer Communications*, 26(13):1504–1514, 2003.

[6] A. A. Pirzada, A. Datta, and C. McDonald. Propagating trust in ad-hoc networks for reliable routing. In *Proc. of IWWAN*, pages 58–62, June 2004.