SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. (2009)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.163

Differentiated security in wireless mesh networks

Thomas Gamer*,†, Lars Völker and Martina Zitterbart
Institute of Telematics, University of Karlsruhe, Germany

Summary

The upcoming IEEE 802.11s standard enables easy establishment and maintenance of wireless mesh networks in residential and enterprise scenarios. They, however, need 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. Copyright © 2009 John Wiley & Sons, Ltd.

KEY WORDS: security; secure routing; traffic differentiation; wireless mesh networks

1. Introduction

Wireless mesh networks currently are standardized by the IEEE 802.11s Task Group [1]. 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. In residential scenarios usually a small number of a house's wireless devices are connected to the Internet using an IEEE 802.11s mesh network. Enterprise scenarios are concerned with bringing connectivity to all the different devices and people in a large company building.

However, many security challenges exist since physical access on the transmission medium cannot be restricted in wireless networks in general. Thus, attacks like eavesdropping, changing frame content, and unauthorized participation in communication are possible if no appropriate security mechanisms are used.

In contrast to the single-hop communication used in IEEE 802.11 [2] wireless networks, IEEE 802.11s 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. An example of such a MAC layer routing protocol is the Hybrid

*Correspondence to: Thomas Gamer, Institute of Telematics, University of Karlsruhe, Germany.
†E-mail: gamer@tm.uka.de

Wireless Mesh Protocol (HWMP) being specified within the scope of the IEEE 802.11s standardization. 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.

Mesh networks can be an alternative to regular wired networks especially when the cost of a wired infrastructure is high. As an alternative, however, they should allow for similar security as wired networks. In large wired networks compartmentalization using Virtual LANs (VLANs) according to the IEEE 802.1Q standard [3] and firewalls are used to increase security. This allows to group nodes of similar kind together, for example all nodes of a department or project team. These nodes can communicate easily with each other while the communication with other nodes can be more strictly controlled. This permits to effectively limit the communication with nodes of other groups and control the exposed services. However, such a compartmentalization cannot be achieved easily in mesh networks.

Due to path selection and multi-hop communication on MAC layer, nodes can influence each other and thus, new attacks become relatively easy. Attackers in these cases are internal malicious nodes that legitimately take part in the mesh network. For instance a node could drop or delay frames of other nodes in a selective forwarding attack. A node might eavesdrop on the communication of his neighbors and on the path selection messages exchanged between them. A node might maliciously influence the routing protocol or directly attack other nodes of the same mesh network. Compartmentalization can mitigate these risks and protects nodes against outsiders. One possible approach for this would be splitting the mesh network into several smaller independent mesh networks. However, this might result in contention for resources and can lead to difficulties for nodes who need to be member of multiple compartments. Such nodes might end up missing important data, management, or signaling frames of one mesh network, while listening to another or might need multiple radios. Therefore, a better solution is needed.

In this paper we present a new approach for compartmentalization of IEEE 802.11s mesh networks, which is called *differentiated security*. We show the cryptographic and security means needed to reach a similar level of security as VLANs offer today, while considering the implications of the wireless medium and layer 2 forwarding in mesh networks. Also, the necessary protocol enhancements are presented and discussed. Furthermore, we integrated the mechanisms of differentiated security into the network simulator ns-2 [4] to prove the feasibility of our concept and show that tools for network planning which support differentiated security can be developed. This enables network administrators to check in advance how their particular wireless mesh network behaves if the intended configuration is applied. We are confident that differentiated security can close the gap between the security of wired networks and IEEE 802.11s mesh networks. This allows mesh networks to become a viable solution even with strong security concerns.

This paper is structured as follows: Definitions of external and internal attackers as well as the attacks we focus on in this paper are explained in the following Section 1.1. The basic concept of differentiated security and an exemplary small enterprise scenario are described in Section 2. Then, Section 3 focuses on the design decisions that were made during development of our solution. A tool that assists network administrators in planning their particular wireless mesh network is presented in Section 4. Finally, related work is discussed in Section 5 before Section 6 gives a conclusion and an outlook on future work.

1.1. Possible Attacks in Mesh Networks

Regarding attacks in wireless networks, we distinguish three basic types of attackers:

- Nodes showing *unintended behavior* due to hardware or software failures: problems caused by such nodes should be solved by fault tolerance mechanisms instead of security mechanisms. Therefore, we will not consider such nodes within this work.
- *External malicious* nodes, which are intentionally not allowed to join the network.
- *Internal malicious* nodes, which legitimately are part of the network and show egoistic behavior or are compromised by an attacker. Egoistic behavior, e. g., intentionally dropping frames, aims at saving resources or gaining higher bandwidth. Attacks could be launched by dropping frames, by corrupting the routing protocol, or by eavesdropping on confidential data.

In this paper we assume that neither external nor internal malicious nodes are able to break the keys and cryptographic algorithms used for protection of the network.

DOI: 10.1002/sec

In the following, we will mainly focus on three attacks.[‡] External malicious nodes are only able to perform the last one, internal attackers may launch all of them:

- *Selective forwarding*—With this active attack, an internal malicious node intentionally drops frames of other nodes that actually should be forwarded by the malicious node. This attack may aim at disrupting a certain communication, a specific node, or just the communication of the wireless network.
- *Routing Attacks*—In case of routing attacks, an internal malicious node tries to influence the routing protocol in a way that incorrect forwarding paths are used. A wormhole attack [6], for example, aims at establishing a route to a victim node even if there are shorter routes. This enables gaining information of specific communications in the network or selectively forwarding frames.
- *Eavesdropping*—If no cryptographic protection is applied within a wireless network, external and internal malicious nodes are able to eavesdrop on the traffic. If some protection like Robust Secure Network (RSN) [2] or IEEE 802.11s security mechanisms is present, internal attackers are still able to eavesdrop on all traffic that is sent within their neighborhood. External attackers, however, are precluded from eavesdropping.

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.

In this way, our approach is able to establish a security level in mesh networks comparable to VLANs in Ethernet networks. VLANs allow for transport of different virtual networks over a single network by tagging the frames. The difference in 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 commonly do not forward frames for other nodes. In mesh networks, nodes have to forward frames and attackers may easily eavesdrop on all links at once.

An easy solution for separation of nodes and traffic would be a partitioning into different mesh networks. Our initial simulations suggest that this can result in reduced network coverage and an increased likelihood of unreachable nodes within each network due to the lower number of participating nodes. More importantly, multiple radios would be necessary if nodes want to participate in multiple networks, e. g., since various communications should be protected differently and may use different wireless channels. Therefore, in our solution, nodes can be assigned multiple protection levels at the same time. Thus, a single mesh network is sufficient.

We propose usage of multiple group keys—one per protection level—in order to achieve differentiated security. Group keys have some advantages over pairwise 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. Furthermore, multicast and broadcast messages can be directly secured with group keys.

2.1. Detailed Example: Small Enterprise Mesh

Figure 1 shows an exemplary small enterprise scenario[§] with eight mesh nodes and one authentication server (AS). Node A is a Mesh Portal Point (MPP). This node provides a connection to the AS 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

[‡] A general overview of attacks in wireless networks is e. g., given in Reference [5].

[§] This is just an examplary scenario. We discuss more complex scenarios in Section 3.3.

DOI: 10.1002/sec

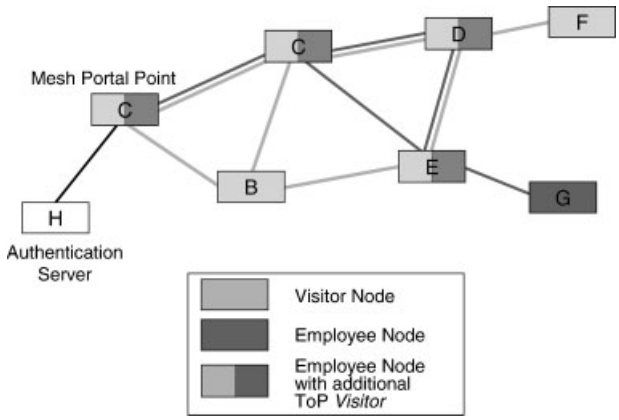

Fig. 1. Exemplary small enterprise scenario.

Wireless LAN (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 what employee nodes get. Since ordering of ToPs would restrict flexibility of ToP mapping too much (see Section 3.3), our concept allows for assignment of multiple independent ToPs to a node. This enables such a node 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. Initial simulation results suggest that with our solution network partitioning and unreachable nodes due to unfavorable number of ToPs or disadvantageous ToP assignment are not impossible but less likely than in multiple separate mesh networks. This is plausible since the density of participating nodes is higher with one instead of multiple networks.

After initial authentication, each node gets its ToPs and the associated group keys from the AS. This authentication prevents external malicious nodes from taking part in the mesh network. Transmission of ToPs and group keys is secured by the Pairwise Master Key (PMK) between authenticating node and AS, 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 internal 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 (see Section 3.1). 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. Design Decisions

In this section, the different design decisions are explained that lead to the proposed solution. First, we focus on assignment of protection levels to frames and the transport of the ToP values within the frames. Then, we briefly consider protection of this value before a suitable ToP mapping is detailed.

3.1. ToP Assignment and Transport

Two fundamental design decisions have to be made: How does the system know which ToP to assign to a given frame and how does a frame transport the ToP value?

The *assignment of ToP values* can be done by using information of different layers, e. g., the application layer or the network layer. A simple solution is to use ToPs like VLAN tags, and assign different ToPs to different network layer addresses, e. g., IP addresses. This can be implemented using virtual interfaces and routing, and is transparent for the application. It can,

DOI: 10.1002/sec

however, lead to increased need of network layer addresses since each node might need a unique address for each protection level it is part of.

Another solution is to let the application select the appropriate ToP and use just one network layer address per node. This approach is more powerful but leaves the application with the problem of assigning the correct ToP—a difficult task for legacy applications. However, these are not the only options. The assignment can be done based on multiple criteria of different layers or applications. The decision how to achieve an optimal assignment depends on the actual scenario the differentiated security should be applied in.

The second design decision is the *transport of the ToP value*, which is needed for the intermediate node to make the correct forwarding decisions. Since mesh networks should be able to transport more than just regular IP traffic, we cannot easily store the ToP value in the network layer or above. That leaves two options for transporting the ToP value in the header of every frame:

- Inside the MAC header
- A shim header right above or below the MAC header

Usage of a shim header, on the one hand, could cause problems during frame processing of nodes that do not know this new header, e. g., legacy IEEE 802.11 stations. In order to store a frame's ToP value inside the MAC layer header, there are several possibilities. One approach is to reuse a field of the original IEEE 802.11 MAC layer header, e. g., the sequence control field. In this case, it is possible that the field is altered by an intermediate node if this node uses the field in its original intention. A node, for example, could take the ToP value of the sequence control field as sequence control number during processing and thus fails. Due to such ambiguities, it is not recommended to store a ToP in an already occupied field of the IEEE 802.11 MAC header. Another approach is to add a new optional field to the header or to use a field that currently is reserved for future use. Since the field is optional or reserved, legacy nodes do not process it and thus, backwards compatibility is ensured. Therefore, we extended the MAC layer frame specified by IEEE 802.11s by an optional field that transports the ToP value.

3.1.1. Extended MAC layer frame format

The header format of MAC layer header in case of mesh networks according to IEEE 802.11s is shown in Figure 2. The differences in comparison to the original IEEE 802.11 header format are highlighted in gray. Due to the multi-hop communication on MAC layer, the 4-address frame format is used by mesh frames. Therefore, the header flags *ToDS* and *FromDS* of the Frame Control field both are set to 1. The IEEE 802.11 standard defines this value combination of flags for future use only. This ensures that only mesh-capable nodes process the frame and the additional mesh header in front of the payload. Legacy IEEE 802.11 nodes, which are not capable of mesh networks and their extensions, only recognize an invalid ToDS/FromDS combination and thus, silently discard the frame. This ensures that legacy nodes do not run into processing problems. The additional mesh header includes a time to live (TTL), Carnegie Mellon University (CMU), wired equivalent privacy (WEP), optimized link state routing (OLSR), secure AODV (SAODV) value and a Sequence Number as well as a Flags field. Currently, only two out of eight bits of the Flags field are defined and used: one indicates whether the Mesh Address Extension field is present and the other indicates which addresses the extension contains.

One of the currently unused bits of the Mesh Flags field now could be used to define a further flag called *ToP*. This flag indicates that a ToP field of one octet

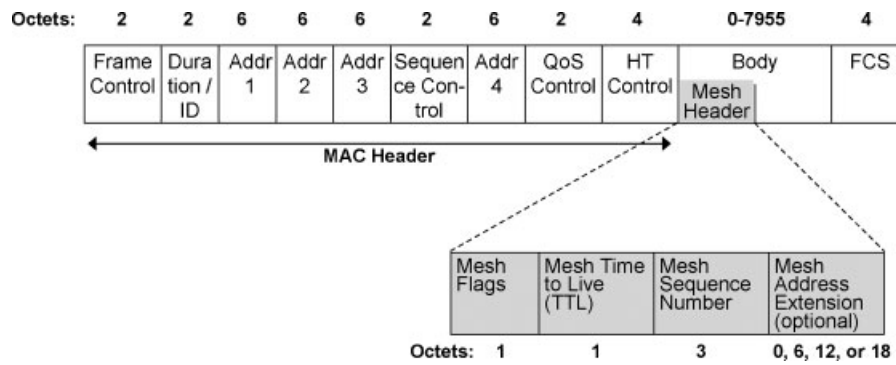

Fig. 2. IEEE 802.11s MAC header format.

DOI: 10.1002/sec

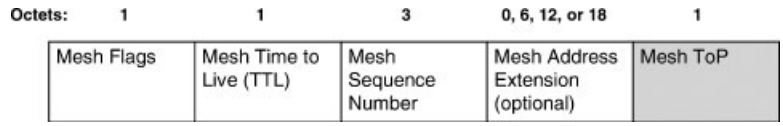

Fig. 3. Extended IEEE 802.11s Mesh header format.

length is added to the Mesh Header subsequent to the Mesh Address Extension field (see Figure 3).

3.2. ToP Protection

Assigning and transporting the ToP within the IEEE 802.11s MAC header enables the differentiated security to function. However, new attacks might be possible, if the new header field is not protected against modification. Attackers could apply address spoofing in order to inject traffic with MAC addresses of legitimate nodes. Furthermore, injection of frames of other ToPs is possible without knowing the correct ToP group key.

In order to avoid these attacks, the integrity of the frame has to be protected by the key associated to the frame's ToP. This can be achieved by adding a new integrity check value (ICV) field to the packet's Mesh Header. This guarantees that nodes, which do not possess the appropriate ToP group key, are not able to create a legitimate frame for this ToP without making the frame invalid due to lack of integrity. All nodes possessing the same ToP as the sending node are still able to execute the attacks previously mentioned. In Section 2 we, however, already stated that differentiated security is not designed to avoid attacks of such nodes.

To make sure that no attacks are possible, every forwarding node must first check the integrity of the frame. Since forwarding changes the frame, e. g., transmission address, mesh TTL, and other fields, two approaches are possible:

- Protect the mutable fields by recalculating the ICV at every hop
- Do not protect the mutable fields and keep the ICV value constant

While the first approach involves less cryptographic calculation and energy consumption, the second approach protects the mutable fields and prevents replay attacks. The replay attacks are based on spoofing the Sequence Control field for replayed frames and can be detected only if this mutable field is protected. Considering current wireless network hardware, we expect that the cryptographic primitives will be implemented in hardware and are able to execute the validation and protection of the frames at the maximum transmission speed. We conclude that the cryptographic overhead and energy consumption for recalculating the ICV at every hop are acceptable for the additional benefit of protection against replay attacks.

3.3. ToP Mapping

Due to the introduction of differentiated security in mesh networks, a suited mapping becomes necessary. In a residential scenario, which only consists of about a dozen of mesh nodes, it is relatively easy to define such a mapping since a very small number of protection levels is sufficient. A trivial mapping is shown in Figure 4. In this example two protection levels exist that are totally ordered. Traffic that is labeled with ToP *Residential* is forwarded only to the nodes of protection level *Residential*. If confidentiality is assured by encryption such traffic cannot be read by nodes of ToP *Visitor*. Frames that are secured by ToP *Visitor* can be forwarded and read by each node of the mesh network—due to the totally ordered protection levels—since each node of ToP *Residential* additionally gets ToP *Visitor*. Thus, residential nodes are trusted more than visitor nodes.

In large enterprise scenarios, two totally ordered protection levels may not be suitable any more. In this case partially ordered protection levels could be used. Figure 5 shows an exemplary mapping. In this scenario, internal traffic of the company has to be protected at least with ToP *Employee*. Traffic labeled with ToP *Visitor* can be forwarded by each node participating in the mesh network. Visitor nodes, however, are only able to read and forward traffic protected by ToP *Visitor*.

A total or partial ordering is advantageous in regard to the mesh network's configuration overhead. If the

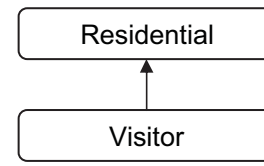

Fig. 4. Totally ordered protection levels in a residential scenario.

DOI: 10.1002/sec

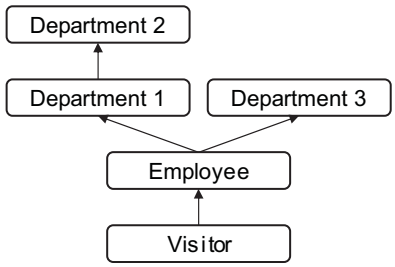

Fig. 5. Partially ordered protection levels in an enterprise scenario.

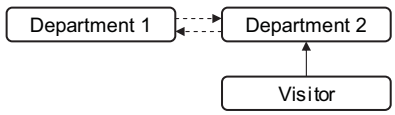

Fig. 6. Unordered protection levels in an enterprise scenario.

protection levels are ordered, the network administrator only has to specify the *most trusted* protection level of a node. Based on the given order, the AS then is able to automatically derive all protection levels that have to be assigned to the node after successful authentication. If no order exists an administrator has to configure all mappings of ToPs to nodes manually.

Due to various threats and different security policies some scenarios do not allow for a partial order at all. Figure 6 shows an example with unordered protection levels. Such an ordering could, for example, be necessary due to resource saving of *Department 1* nodes. Therefore, a protection level mapping must not require any order of protection levels. This ensures high flexibility of differentiated security. Since protection levels used in mesh networks highly depend on external factors, like the structure of the enterprise, no universal protection level definitions can be given.

4. Simulation Study

Network administrators and designers planning to use differentiated security in wireless mesh networks need to be aware of design decisions, especially the allocation of ToPs. We are confident that current tools for wireless network planning, like for example Reference [7], can be easily enhanced to support our approach. To prove the feasibility of such a modification, we have implemented our concept with the ns-2 [4], and used this for evaluation of different ToP allocation schemes. While ns-2 is not suitable as a network planning tool for administrators, it allowed us to show that our approach as well as a network planning tool for it works as expected. The following details of our implementation should document this.

In the regular ns-2 a slightly simplified implementation of the IEEE 802.11 MAC layer is included. Based on this default MAC layer model, we had to implement functionality of wireless mesh networks for ns-2 as first step. As a second step, we added the functionality necessary for differentiated security.

a) *Integration of mesh functionality into MAC layer*: Major changes to the default MAC layer were needed because mesh networks introduce multi-hop communication on MAC layer, implementation of frame forwarding, duplicate detection, and other related features. In order to support MAC layer routing protocols, we decided to integrate an additional layer—the mesh routing layer—into the ns-2 model of a mobile node according to the CMU monarch's wireless extension to ns [8]. Figure 7 shows the resulting model. The `MeshRouting` layer receives all routing messages from MAC layer (`mesh_`), processes these messages, and calculates the node's mesh forwarding table. Furthermore, it creates its own routing messages and inserts them into MAC layer sending queue (`target_`). The addition of a separated mesh routing layer into the ns-2 model ensures simple exchange of the used mesh routing protocol and easy extension and adaptation of mesh functionalities.

We additionally implemented a proprietary proactive MAC layer routing protocol, which was developed within the scope of the Siemens Campus Project, into

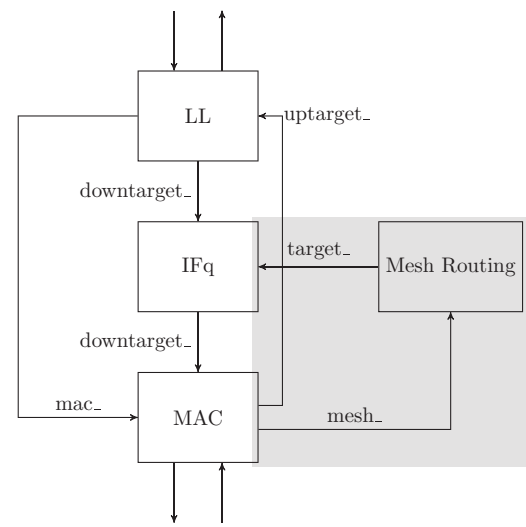

Fig. 7. Extension of the ns-2 model by an additional mesh routing layer.

DOI: 10.1002/sec

the resulting MAC/Mesh layer model. In summary, our MAC/Mesh layer implementation for ns-2 includes all mechanisms necessary for multi-hop communication on MAC layer as well as a proprietary proactive MAC layer routing protocol.

b) *Integration of security entities for authentication*: In order to allow for authentication of mesh nodes a special node, the AS, was integrated into the simulation environment. The AS is configured by an access control list, which contains the nodes that are allowed to join the mesh network as well as protection levels each node belongs to after authentication. For simplification, an authentication procedure consists of a 4-way handshake. Within the last message of such a handshake, the AS transmits ToPs as well as associated group keys to the supplicant.

Mesh nodes, that are already authenticated, periodically send beacon messages in order to announce the mesh network. A new node can join the network by sending an authentication request to such an announcing node. Since messages can be sent only to already authenticated nodes, which take part in the MAC layer routing protocol, the announcing mesh node has to act as authenticator, i. e., as proxy node, for the supplicant. This is achieved by tunneling the frames to and from the AS.

c) *Integration of protection levels and associated mechanisms*: In order to apply differentiated security to a wireless mesh network, traffic has to be assigned a ToP. In our implementation ToP assignment is left to applications. The ToP of an application can be set in within an ns-2 simulation configuration file by

set `cbr [new Application/Traffic/CBR]`
`$cbr` **set** `mesh_top_1`

This example sets the ToP of constant bitrate traffic (CBR) generated by a specific node to 1.

All mesh nodes, participating in the mesh network, take part in MAC layer routing. Due to the application of differentiated security a multi-path routing is achieved by applying a routing protocol for each ToP separately. Routing messages are protected by the ToP group key.

The overhead introduced by running one routing protocol per ToP is neglectable for reactive routing protocols like HWMP as long as the compartmentalization does not lead to additional communication. For proactive routing protocols, however, the overhead depends on the number of ToPs (m) used in the mesh network as well as the average number of ToPs a node is assigned to. In the worst case every node is assigned to every ToP; thus, leading to an overhead and signaling burden equal to the number of ToPs. However, this case should never be encountered in real world networks because security would not be increased—this situation conflicts with the design goals for a mesh network with differentiated security.

Even so, proactive routing overhead could be optimized by using a single modified routing protocol for all ToPs at once. This requires the routing messages to be authenticated using all applicable ToPs and does not allow for encryption. Furthermore, route filters need to be used to delete routes conflicting the ToP topology.

4.1. Simulation-supported Network Planning

With differentiated security it is possible to compartmentalize mesh networks and thus, achieve security comparable to VLANs in wired networks. In contrast to VLANs, however, one has to overcome the problems introduced by the wireless medium when using differentiated security in wireless mesh networks. In addition, mobility and multi-hop communication further complicate things in wireless networks. Therefore, one has to make sure that using differentiated security does not lead to partitioning of the mesh network and that the medium is used efficiently. In order to cope with these problems a network planning tool should be used. Only minor modifications have to be made to such a tool in order to support differentiated security. The following simulations were used as feasibility study.

Based on the implementation of differentiated security into ns-2, we exemplarily simulated two different scenarios: residential and medium enterprise. The exemplary *residential scenario* consisted of eight mesh nodes. Positioning of nodes was performed randomly within an area of 500 m × 500 m. In our simulation the nodes showed no mobility. Node mobility, however, could be easily added, e. g., by using a mobility generator like BonnMotion [9]. Differentiated security was based on two ordered protection levels. All eight nodes belonged to ToP 0, ToP 1 was randomly assigned to nodes. In the first simulation, a large number of nodes belonged to ToP 1. The resulting scenario is shown by Figure 8. In a second simulation, only a small number of nodes—nodes 0, 4, and 6—belonged to ToP 1. In both simulations the mesh network showed the intended behavior: packets of each protection level are secured by the according ToP group keys and all nodes of each protection level are able to communicate with each other. Attacks of authenticated nodes that are not part of the respective protection level are not possible any more. It is,

DOI: 10.1002/sec

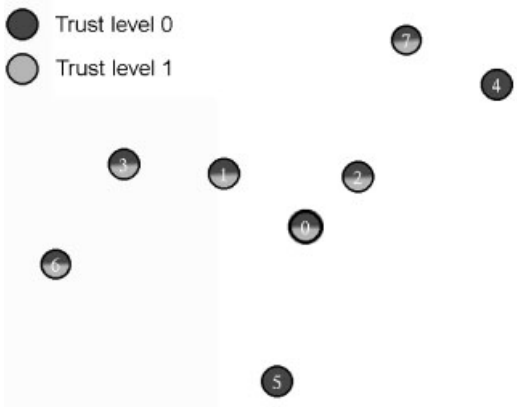

Fig. 8. Residential simulation scenario.

however, observable that less alternative routing paths exist within a single ToP in comparison to available routing paths regarding all participating nodes. In the latter scenario, for example, only a single path exists between nodes 4 and 6 for ToP 1 whereas for ToP 0, nodes 0, 1, or 2 could additionally serve as forwarding node for a communication between nodes 4 and 6. The reduced number of routing paths is caused by the fact that only a subset of all nodes takes part in each compartment of the mesh network. This situation, however, would not improve if multiple networks are used instead of our differentiated security approach.

There are also scenarios that show a single unreachable node or a partitioning of the network within a certain protection level. If, for example, nodes 4, 5, and 7 belong to ToP 1, there exists no path between nodes 4 or 7, respectively, and node 5—node 5 is unreachable within ToP 1. This situation is not caused by usage of our compartmentalization approach but by unfavorable network planning—even if separated networks would be used, node 5 would still be unreachable.

The exemplary *enterprise scenario* consisted of 30 nodes within an area of 1000 m $\times$ 1000 m and was based on four trust levels that were randomly assigned to nodes: 18 nodes belong to ToP 0, seven to ToP 1, 14 to ToP 2, and 13 to ToP 3. In this scenario an unordered ToP mapping was applied. Again, no connection problems occurred during the simulation. In a second simulation only eight nodes were assigned to ToP 2. In this simulation partitioning of the mesh network occurred within ToP 2. In case of partitioning, no communication is possible between nodes of different partitions within the affected protection level. A further simulation was conducted with a different random positioning of nodes and the the same distribution of protection levels. In this simulation a single node of ToP 3 was not reachable any more within this ToP—ToP 2, however, showed no partitioning with this changed setup.

From these exemplary results, it is observable that good network coverage and reachability of the nodes in every compartment heavily depend on the scenario differentiated security is applied in. Unfortunately, there is no rule of thumb giving advice on a suitable number of protection levels in a mesh network since this depends on the semantics of the network. An approximation of the number of nodes per protection level that are necessary to avoid partitioning can e. g., be calculated based on the findings of Bettstetter [10].

As expected, our simulation results did not show any differences in regard to partitioning compared to a scenario with multiple parallel mesh networks, in which nodes take part in multiple of these networks at once. Hence, one could think of a mesh network with differentiated security as just a couple of parallel mesh networks with nodes being part in multiple of such networks. However, our approach allows nodes with a single wireless radio to be part of different mesh networks at once and still have higher security as a single network.

Using a modified wireless network planning tool for mesh networks with differentiated security mesh network administrators could check applicability of differentiated security in their actual planned mesh network before deployment, like we were able to by using ns-2.

5. Related Work

Mechanisms like hiding of an IEEE 802.11 infrastructure network's Service Set Identifier (SSID) or application of a MAC address filter are frequently used to secure wireless networks. These mechanisms, however, are not difficult to overcome [11]. Therefore, cryptographic mechanisms like encryption of wireless communication have to be applied in order to achieve access control in wireless networks. In case of WEP encryption [2] only nodes that possess an appropriate preshared key are able to take part in the communication. Unfortunately, there exist numerous attacks on WEP which result in the fact that unauthorized nodes can obtain the secret preshared key without too much effort [12]. Thus, RSN [2] should be used in order to secure a wireless network against external attackers. This security mechanism achieves confidentiality by using the Advanced Encryption

DOI: 10.1002/sec

Standard (AES) [13] and avoids failures of WEP, e. g., bad choice of initialization vectors (IV). Authentication and key distribution in large enterprise networks in the majority of cases is achieved by an AS using IEEE 802.1X [14] in combination with e. g., RADIUS [15]. In residential and small enterprise scenarios, nodes are mostly authenticated based on preshared keys. IEEE 802.11s security [1] is based on RSN and proposes an extended key hierarchy with an additional indirection level. Cryptographic protection within differentiated security is built on some of these basic security mechanisms for protection of data traffic.

In addition to the mechanisms for protection of data frames, there exist similar mechanisms for protection of management frames and routing messages. IEEE 802.11w [16], for example, has recently been ratified specifying mechanisms for protection of IEEE 802.11 MAC layer management frames. Protocols like Secure OLSR [17] and SAODV [18] allow for a protection of routing protocols on network layer, e. g., in IEEE 802.11 *ad hoc* networks. Such protocols, however, cannot prevent internal malicious nodes from launching attacks like selective forwarding, influencing routing paths, or eavesdrop on forwarded data. Furthermore, they require pre-distributed pairwise keys for protection.

The security architecture MobiSEC [19] offers protection of all the traffic sent in a wireless mesh network. The framework builds on existing protocols, e. g., IEEE 802.11i, to achieve access control and key distribution. Authentication is based on asymmetric cryptography, i. e., on client certificates. Protection of the subsequent wireless communication relies on group keys. Additional protection is provided by separating access control of mesh users from mesh routers. Insider attacks like selective forwarding performed by an already authenticated router, however, cannot be prevented by this security architecture. To achieve a differentiation of nodes, e. g., to separate visitors from employees, two mesh networks have to be established, which then can be secured using MobiSEC.

Solutions like those given in Reference [20,21] try to avoid selective forwarding by rewarding correct behavior using virtual currency. Other approaches try to detect such behavior by using a reputation-based approach [22,23]. Trust-based routing mechanisms in *ad hoc* networks, e. g., Reference [24] or Reference [25], try to avoid forwarding frames to malicious nodes by observing, rating, and distributing or utilizing, respectively, 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 and error-prone based on meta knowledge than with dynamically calculated trust levels or reputation values.

One of the approaches, very similar to our work, is VLANs [3] for IEEE Ethernet Networks. VLANs allow for transport of different virtual networks over a single network by tagging the frames according their VLAN. The major difference to our work is the different attacker model and that we are using a wireless mesh network instead of wired Ethernet. Therefore, a solution for wireless mesh networks requires advanced cryptographic concepts.

6. Conclusions

In this paper we presented a security concept for wireless mesh networks similar to a cryptographically protected VLAN. Cryptographic protection is necessary in wireless networks since each node is able to eavesdrop on traffic or to inject own traffic due to the characteristics of the transmission medium. By assigning specific ToP to each participating node, a separation of data traffic and routing into different protection levels is achieved. This prevents attacks of internal nodes, e. g., selective forwarding or eavesdropping on confidential data. This is very important especially in enterprise scenarios where e. g., visitors are able to use the same WLAN mesh as employees.

On the one hand, certain ToPs are assigned to each participating node after successful authentication. On the other hand, traffic is assigned a certain ToP, e. g., by applications or usage of virtual interfaces. After that, MAC layer frames are marked with the ToP they are protected with and forwarded to trusted nodes only. Payload data can be encrypted according to the ToP group key. Furthermore, these keys can be used for differentiated protection of management frames. This avoids attacks of external nodes as well as internal nodes that do not posses the appropriate ToP group key. Finally, we integrated our solution into the ns-2. This did not only allow us to validate our solution but also acted to prove the feasibility of a network planning tool for mesh networks using differentiated security. Such a network planning tool easily allows network administrators to check the behavior of their specific wireless mesh scenario in regard to their intended ToP configuration.

DOI: 10.1002/sec

Differentiated security combines the security benefits of compartmentalization with the management advantages of a single large mesh network. Users only have to join and authenticate to a single mesh network and are automatically assigned appropriate ToPs; thus, being protected while communicating.

In future work, applicability of differentiated security in real mesh networks should be evaluated in already deployed residential and enterprise meshes. This could give valuable insights into reasonable selection of the number of protection levels and the assignment of available ToPs to mesh nodes in specific scenarios. Lastly, the integration of legacy IEEE 802.11 stations—which can be associated to mesh access points and thus, participate in a mesh network—into differentiated security should be considered.

Acknowledgements

The authors gratefully acknowledge that this work was funded by Siemens Enterprise Communications GmbH & Co. KG within the scope of the Siemens Campus Project. The authors would also like to thank especially Michael Bahr, Rainer Sauerwein, and Jürgen Totzke for valuable discussions and scientific advice throughout the project.

References

1. IEEE Draft Standard for Information Technology—Telecommunications and information exchange between Systems—Local and metropolitan area Networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 10: Mesh Networking. IEEE P802.11s/D3.04, October 2009.
2. IEEE Draft Standard for Information Technology—Telecommunications and information exchange between Systems—Local and metropolitan area Networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2007, June 2007.
3. IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks. IEEE Std 802.1Q-2005, May 2006.
4. The Network Simulator ns-2, Version 2.29.2. Available at: http://www.isi.edu/nsnam/ns/ [December 2005]
5. Welch D, Lathrop S. Wireless security threat taxonomy. In *Proceedings of Information Assurance Workshop*, June 2003; 76–83.
6. Deng H, Li W, Agrawal D. Routing security in wireless *ad hoc* networks.*IEEE Communications Magazine* 2002; **40**(10): 70–75.
7. García MM, Fernandez-Durán A, Alonso JI. Automatic planning tool for deployment of indoor wireless local area networks. In *IWCMC '09: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing*. New York, NY, USA: ACM, 2009; 1428–1432.
8. Fall K, Varadhan K. The ns Manual. Available at: http://www.isi.edu/nsnam/ns/ns-documentation.html [August 2000]
9. Gerharz M, de Waal C. Bonnmotion—a mobility scenario generation and analysis tool. Available at: http://web.informatik.uni-bonn.de/IV/BoMoNet/BonnMotion.htm [October 2005].
10. Bettstetter C. On the connectivity of *ad hoc* networks. *The Computer Journal* 2004; **47**(4): 432–447.
11. Arbaugh W, Shankar N, Wan Y, Zhang K. Your 80211 wireless network has no clothes. *IEEE Wireless Communications* 2002; **9**(6): 44–51.
12. Tews E, Weinmann R-P, Pyshkin A. Breaking 104 Bit WEP in less than 60 seconds. In *8th International Workshop on Information Security Applications (WISA)*, August 2007; 188–202.
13. Daemen J, Rijmen V. Advanced Encryption Standard (AES), Katholijke Universiteit Leuven/ESAT, FIPS 197, November 2001.
14. IEEE Computer Society. *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*, December 2004.
15. Rigney C, Willens S, Rubens A, Simpson W. Remote authentication dial in user service (RADIUS). *IETF, RFC 2865*, June 2000.
16. IEEE Draft Standard for Information Technology—Telecommunications and information exchange between Systems—Local and metropolitan area Networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Protected Management Frames Amendment. IEEE 802.11w-2009, September 2009.
17. Clausen T, Baccelli E. Securing OLSR problem statement. *IETF, Internet Draft*, October 2005.
18. Zapata MG. Secure *ad hoc* on-demand distance vector (SAODV) routing. *IETF, Internet Draft*, September 2007.
19. Martignon F, Paris S, Capone A. Design and implementation of mobisec: a complete security architecture for wireless mesh networks. *Computer Networks* 2009; **53**(12): 2192–2207.
20. Buttyan L, Hubaux J. Nuglets: a virtual currency to stimulate cooperation in self-organized mobile *ad hoc* networks, *ICCA, Swiss Federal Institute of Technology*, 2001.
21. Lamparter B, Paul K. Westhoff D. Charging support for *ad hoc* stub networks. *Computer Communications* 2003; **26**(13): 1504–1514.
22. Kraft D, Schäfer G. Distributed access control for consumer operated mobile *ad hoc* networks. In *Proceedings First IEEE Consumer Communications and Networking Conference*, 5–8 January 2004; 35–40.
23. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile *ad hoc* networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*. ACM, 2000; 255–265.
24. Pirzada A, Datta A, McDonald C. Trust-based routing for *ad hoc* wireless networks. In *Proceedings of 12th IEEE International Conference on Networks (ICON)*, November 2004; 326–330.
25. Ghosh T, Pissinou N, Makki K. Towards designing a trusted routing solution in mobile *ad hoc* networks. *Mobile Networks and Applications* 2005; **10**(6): 985–995.

DOI: 10.1002/sec