WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. **00**: 1–25 (2008)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/wcm.0000

Securing Multi-operator Based QoS-aware Mesh Networks: Requirements and Design Options

I. Askoxylakis[1], B. Bencsáth[2], L. Buttyán[2]*, L. Dóra[2], V. Siris[1], D. Szili[2], I. Vajda[2]

[1]*Institute of Computer Science*
Foundation for Research and Technology Hellas (FORTH)
P.O. Box 1385, GR 711 10, Heraklion, Crete, Greece

[2]*Laboratory of Cryptography and System Security (CrySyS)*
Budapest University of Technology and Economics
Magyar tudósok krt 2, H-1117 Budapest, Hungary

Summary

Wireless mesh networking allows network operators and service providers to offer nearly ubiquitous broadband access at a low cost to customers. In this paper, we focus on QoS-aware mesh networks operated by multiple operators in a cooperative manner. In particular, we identify the general security requirements of such networks and we give an overview on the available design options for a security architecture aiming at satisfying those requirements. More specifically, we consider the problems of mesh client authentication and access control, protection of wireless communications, securing the routing, key management, and intrusion and misbehavior detection and recovery. Our aim is to structure this rich problem domain and to prepare the grounds for the design of a practically usable security architecture. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: Wireless mesh networks, Authentication, Secure routing, Secure communications, Key management, Intrusion detection and recovery

1. Introduction

Mesh networks [1, 2] represent an emerging wireless networking technology that promises wider coverage than traditional wireless LANs and lower deployment cost than 3G cellular networks. For these reasons, network operators and service providers consider mesh networking to be a serious candidate to solve the so called "last mile problem". Indeed, at many places in the world, some network operators have already started to deploy mesh based solutions offering nearly ubiquitous and inexpensive wireless Internet access to their customers. Examples for this development include Ozone's mesh network in Paris (www.ozone.net/en/) and *The Cloud* in the City of London (www.thecloud.net). If these pilot projects turn out to be successful, then mesh networking may become extremely popular and wide-spread.

While there also exist so called community based mesh networks that are operated by individuals, we believe that the real business potential lies in operator based mesh networks. By their systematic design, deployment, and maintenance, operator based mesh networks provide higher level of Quality-of-Service

*Correspondence to: buttyan@crysys.hu

(QoS), meaning larger scale coverage, higher speed, and more reliable operation. In addition, it can be envisioned that mesh network operators in a given geographical area will cooperate in order to further optimize their costs and increase the QoS provided by their networks. The form of the cooperation can range from traditional roaming agreements to joint provision of specific services. This kind of cooperation is less likely to happen between ad hoc communities. Hence, in this paper, we focus our attention on QoS-aware mesh networks operated by multiple operators.

In order to turn the tremendous business potential represented by mesh networking into real profit, one needs to solve a number of technical problems related to the design and operation of mesh networks. In this paper, we address one of those problems: securing mesh networks. It is evident that security issues need to be considered seriously and solved appropriately. The reason is that, due to the wireless nature of the communication medium, and due to the lack of physical protection of the unattended mesh nodes, it is relatively easy to carry out various attacks against mesh networks. Furthermore, if security is not handled appropriately, then the customers may prefer alternative technologies; this would hinder the adoption and wide-spread deployment of mesh networks, which in turn, would result in loss of business opportunities.

More specifically, in this paper, we identify the security requirements that are relevant for wireless mesh networks in general, and for multi-operator based QoS-aware mesh networks in particular. We understand that security issues are often application specific; however, here we are focusing on the general security requirements of wireless mesh networks that are either independent of the applications or common to all applications. In addition to identifying the security requirements, we also present various design options for a security architecture that aims at satisfying those requirements.

Discussion of the security issues in wireless mesh networks can be found in [3, 4, 5]. However, none of those works address specifically QoS aware mesh networks operated by multiple operators, neither they deal with proactive (cryptographic) and reactive (intrusion detection based) security measures in a combined manner as we do in this paper. The discussion in [3] focuses on giving an overview of the various authentication mechanisms and secure routing protocols proposed for mobile ad hoc networks. Unfortunately, it is very much centered around academic proposals with little practical relevance. Moreover, the mechanisms and protocols proposed for mobile ad hoc networks are useful, but they are not suitable for direct application in mesh networks. The authors of [4] discuss three specific security problems in wireless mesh networks: the detection of compromised mesh routers, the security of routing, and the problem of fairness. These are important problems, but they represent only a somewhat arbitrary subset of the security issues in wireless mesh networks. Finally, the discussion in [5] is specific to wireless mesh network security and it is quite comprehensive in terms of identified security issues. Indeed, the security requirements that we identify in this paper are more or less the same as those identified in [5]. Our contributions that make this paper different from [5] include a more detailed discussion of the available design choices for authentication and network access control, for the protection of wireless communications, and for intrusion and misbehavior detection, as well as a more QoS specific discussion of the routing security problem. Another difference is that, in this paper, we focus on multi-operator based mesh networks, while [5] discusses other scenarios too.

The organization of the paper is the following: First, we introduce our system model in Section 2 and our adversary model in Section 3. Based on these models, we identify the general security requirements in Section 4. Next, we present design options for the elements of a security architecture that aim at satisfying the identified security requirements. More precisely, we address mesh client authentication and network access control in Section 5, protection of wireless communications in Section 6, security of routing in Section 7, key management issues in Section 8, and intrusion and misbehavior detection and recovery in Section 9. Finally, we conclude the paper in Section 10.

2. System model

A detailed survey on mesh network architectures can be found in [1]. In this paper, we consider the following model (see also Figure 1 for illustration): A mesh network consists of mesh routers that form a static wireless ad hoc network. Some of the mesh routers function as gateways to the wired Internet, and some of them function as wireless access points where mobile mesh clients can connect to the network. The sets of gateways and access points can overlap and they do not necessarily cover the entire set of mesh routers.

DOI: 10.1002/wcm

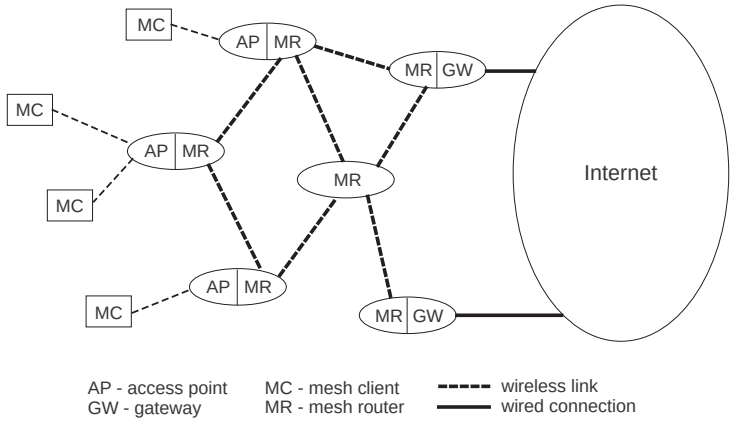

Fig. 1. Illustration of a mesh network.

As shown in Figure 1, we assume that the mesh clients connect to the access points directly (i.e., mesh clients are one hop away from the mesh network). In theory, mesh clients could provide data forwarding services to each other, and connect to the access points via multiple other mesh clients, but this would require special software on the mesh clients (essentially they would function as a router). In practice, however, users may not be willing to modify their mesh clients and to behave cooperatively, and for this reason, we do not consider this possibility of connecting to the access point through multiple mesh clients.

The mesh routers are operated by multiple operators, and we assume that they cooperate in the provision of networking services to the mesh clients. This cooperation is based on business agreements (similar to roaming agreements in the case of cellular networks). Mesh clients are mobile computers operated by customers. Customers may be associated with one or more operators by contractual means.

Mesh clients use the services provided by the mesh network in order to run various applications. Typically, mesh clients use the mesh network to access the Internet, or they run applications that take advantage of the connectivity provided by the mesh network itself (e.g., mesh clients can communicate with each other through the mesh routers without accessing the Internet).

The mesh network supports QoS-based applications and mobility of the mesh clients. In other words, we assume that appropriate mechanisms are used within the network to provide services with QoS guarantees (e.g., the routing protocol uses QoS-aware routing metrics, and it may use admission control and resource reservation mechanisms too), and to ensure seamless handover between access points for the mobile mesh clients. We are not considering the details of these mechanisms; we are interested only in their general security requirements.

3. Adversary model

As usual, the first step in the identification of security requirements is the understanding of the potential attacks against the system. This understanding is summed up in the following adversary model that describes the classes of attackers, their objectives, and their means to attack the system.

Classes of attackers. Taking into account the system model described above, we can identify three types of attackers:

- *External attackers:* These are attackers that have no legitimate access to the mesh network and its services, but they have appropriate equipment to use the wireless medium and interfere with the operation of the mesh network protocols. In addition, these attackers may have unsupervised physical access to some of the mesh routers that are installed in public areas, and they have the knowledge to modify the behavior of these routers by installing rogue software on them.
- *Dishonest customers:* These are misbehaving end-users that have legitimate access to the mesh network services and try to take advantage of this in order to interfere with the operation of the network or to gain illegal access to

DOI: 10.1002/wcm

its services (e.g., by impersonating another customer).
- *Dishonest operators:* These are operators of the mesh infrastructure that do not honestly stick to business agreements.

Objectives of attacks. We identify the following main objectives of attacks:

- *Unauthorized access to the services provided by the mesh network (e.g., Internet access):* Primarily, this objective is relevant for external attackers and dishonest customers. In the latter case, the dishonest customer may try to use services that are not included in his subscription.
- *Unauthorized access to customer data and meta-data:* Here customer data means the content of the messages exchanged in a service session, whereas meta-data refers to information on the customer's location and service usage profile (e.g., which applications are used and how often). Thus, the first objective is related to violating the confidentiality, and the second is related to violating the privacy of the customer. Primarily, this objective is relevant for external adversaries and dishonest operators.
- *Denial-of-Service (DoS):* This objective is related to degrading the QoS offered by the network (including the complete disruption of services). Primarily, this is relevant for external adversaries.
- *Gaining advantage over competitors:* For dishonest operators, the primary reason to mount attacks on the system (especially on those parts that are operated by other operators) is to gain some advantage over their competitors. This is achieved either by destroying the reputation of a competitor, or by dishonestly increasing one's own good reputation.

Attack mechanisms. There are a multitude of attack mechanisms that can be used and combined in order to reach the goals described above. However, most of these mechanisms fall into either one of the following two categories:

- Attacks on wireless communications (including eavesdropping, jamming, replay, and injection of messages, and traffic analysis);
- Setting up fake mesh routers or compromising existing mesh routers (typically by physical tampering or logical break-in). The behavior of the fake or compromised mesh routers can be arbitrarily modified in order to help to achieve specific attack objectives.

4. Security requirements

Based on the adversary model described above, we can identify the following main security requirements for wireless mesh networks:

Authentication of mesh clients and access control. In order to prevent unauthorized access to services, mesh clients must be authenticated, and access control rules must be enforced in the system. Ideally, access control enforcement should take place at the access points such that unauthorized access attempts are denied as early as possible without affecting the rest of the network. There are many options to satisfy this requirement in terms of available authentication protocols and authorization schemes. However, there are additional requirements that need to be satisfied, which may exclude some of those options. These requirements include the need to support end-user mobility and QoS-aware applications, and the need to work in a multi-operator environment.

Supporting user mobility and QoS-aware applications means that re-authentication of mesh clients and access authorizations should be fast such that the requirements of authentication and access control do not exclude the possibility of seamless handover between the access points. In addition, the multi-operator environment means that such handovers may occur between access points belonging to different administrative domains, and hence, the authentication and access control scheme must be able to handle this situation.

Protection of wireless communications. Wireless communications between mesh clients and mesh routers, as well as among mesh routers and gateways must be protected against various attacks. This leads to the following requirements:

- The confidentiality and the integrity of the application data must be protected in order to prevent unauthorized access to user data. This can be done in an end-to-end manner, however, some applications may not be prepared for this protection, in which case, it is desirable to solve the problem transparently to the applications within the mesh network itself.

DOI: 10.1002/wcm

- Message integrity and authenticity must be provided ideally in a link-by-link manner such that fake, modified, and replayed messages are identified and removed as early as possible, and therefore, they do not waste the bandwidth of the network.
- Traffic analysis must be prevented as much as possible in order to prevent unauthorized access to meta-data of the customers, and hence, to ensure some degree of privacy. Link-by-link encryption of messages can help in this matter, as it can hide end-to-end addressing information. In addition, dummy traffic can be maintained by neighboring mesh routers on idle links in order to prevent the identification of communication profiles.

Increasing the robustness of the networking mechanisms. The easiest way to mount stealth DoS attacks against a network is to manipulate its basic mechanisms such as the routing protocol, the medium access control scheme, the topology control and channel assignment mechanisms, etc. For this reason, it is important to increase the robustness of these basic networking mechanisms. In particular, securing the routing protocol seems to be the most important requirement in this category, because interfering with the routing protocol may affect the entire network, whereas attacks on lower layers (e.g., on medium access control and channel assignment) seem to have a localized effect.

In general, QoS-aware routing protocols provide three functions: (1) proactive dissemination of routing information (e.g., link quality metrics) and local route computation, or on-demand route discovery (depending on the type of the protocol), (2) resource reservation on selected routes (for the purpose of QoS guarantees), and (3) recovery from errors during the data forwarding phase.

All of these three functions have their security requirements. Routing information dissemination and route discovery requires the authentication and integrity protection of routing control messages, in order to prevent their manipulation by external adversaries. In addition, in some protocols, special attention must be paid to the protection of non-traceable mutable information (e.g., the cumulative routing metric values) in routing control messages against misbehaving mesh routers. It may also be desirable to ensure non-repudiation of routing control messages in order to discourage operators to mount stealth attacks against each other, and to facilitate dispute resolution.

Resource reservation messages must also need to be authenticated in order to avoid resource blocking DoS attacks. Similarly, it must be guaranteed that resources do not stay reserved forever. Finally, error recovery procedures should not be exploitable by attacks aiming at the disruption of communication or increasing the message overhead in the network.

Intrusion and misbehavior detection and recovery. Due to the fact that our adversary model allows for dishonest operators and physical tampering of mesh routers by external attackers, we must assume that some fraction of the mesh routers may exhibit arbitrary (also called Byzantine) behavior. It is more or less impossible to identify such misbehaving nodes by cryptographic means. Similarly, cryptographic solutions are ineffective against jamming attacks. Therefore, besides the proactive security measures that we have described above, one must also consider the application of some reactive measures aiming at the detection and recovery from attacks based on intrusion and misbehavior.

As misbehavior can happen at any layer of the communication stack, misbehavior detection should be implemented in all layers; moreover, various misbehavior detection modules can be combined in a cross layer approach to increase the effectiveness of the detection. Misbehavior detection and recovery requires that the nodes can monitor the activity of each other (at least to some extent), that they can identify suspicious activities, and that they can make counteractions (e.g., they can exclude misbehaving nodes from the network). This also means that some level of cooperation must take place between the nodes.

Key management. Some of the security requirements that we identified in this section (in particular, mesh client authentication and access control, protection of wireless communications, and some aspects of increasing the robustness of the basic networking mechanisms such as routing) are most conveniently satisfied by using some cryptographic mechanisms. Cryptographic mechanisms, in turn, require cryptographic keys and key management solutions.

More specifically, cryptographic protection mechanisms in mesh networks may require the establishment of shared symmetric keys between various entities

DOI: 10.1002/wcm

(e.g., between mesh routers, between an authentication server and an access point, etc.) and the distribution of the public keys of various entities (e.g., mesh routers, authentication servers, etc.). Both of these can be supported by a public key infrastructure (PKI) established and maintained by the mesh network operators. Moreover, given that we are considering a multi-operator environment where security associations are often established between entities that belong to different administrative domains, a PKI based key management approach seems to be the conceptually simplest and most convenient solution.

5. Authentication of mesh clients and access control enforcement

In a business driven mesh network, it is essential that only authorized users can access the network. To fulfill this requirement, authentication and access control enforcement is required. In the authentication process, the mesh client proves its identity using an authentication key. In addition, during the authentication process, a short-term connection key is established between the mesh client and the access control enforcement point. This connection key serves as the basis for access control enforcement on the follow-up traffic originating from the mesh client.

In this section, we first introduce a detailed list of requirements for authentication and access control enforcement in QoS aware multi-operator maintained mesh networks. Then, we give an overview of the authentication and access control enforcement mechanisms proposed for WiFi and mesh networks, and we analyze them with respect to the identified requirements.

5.1. Requirements

The main requirements for authentication and access control enforcement in a QoS aware multi-operator maintained mesh network are the following:

- *Fast authentication method to support user mobility:* As a main requirement, the authentication method has to support mobility of mesh clients which may use QoS aware services (e.g. VoIP). Such services may have requirements on the length of the interruptions in the communication that they can tolerate. When a mesh client moves from one access point to another, it has to re-authenticate itself as part of the handoff process. Before a successful authentication process the mesh client should not be allowed to access the network (otherwise, it can exploit by changing the access points and gaining access without authentication). Thus, the re-authentication delay must be minimized in order to ensure that the interruption caused by the handoff remains tolerable for the applications.
- *Connection keys should not reveal long term keys:* The connection keys that the access points obtain during the authentication of the mesh clients should not reveal any long-term authentication keys. This requirement must hold because in the multi-operator environment, the mesh clients may associate to access points operated by foreign operators.
- *Independence of connection keys:* As the neighboring access points may not trust fully each other due to the multi-operator environment, the authentication and the key generation mechanism have to prevent an access point from deriving connection keys that are used at another access point.
- *Freshness:* It must be ensured for both participants that the connection key derived during the authentication process is fresh.
- *DoS resistance:* The authentication method should not create any vulnerabilities to DoS attacks. Note, that a successful attack against a central unit (e.g. central authentication server) may lead to a state where no handoff can be completed.
- *Compatibility with standards:* In a multi-operator environment, it is fundamental that the protocols used in the authentication mechanism are standardized or built from standardized elements. Otherwise a mesh client will not be able to authenticate itself at an access point belonging to another mesh operator.
- *Scalability:* One of the main advantages of mesh networks is the increased coverage. This, however, usually means an increased number of mesh routers, access points, and mesh clients. Therefore, the authentication method must be scalable in terms of the number of access points and mesh clients.
- *No single trusted entity:* In a multi-operator environment, no single trusted entity may exist. Hence, each operator should run its own authentication server(s), but those could cooperate with the servers of other operators based on business agreements.

DOI: 10.1002/wcm

5.2. Proposed methods

Taxonomy. In the literature, many authentication and access control enforcement methods have been proposed. We categorize them by the place of the access control enforcement and by the place and type of the authentication.

The access control can be enforced at the following places:

- *Central access control enforcement:* In this case, the access control enforcement is done outside of the mesh network by a special entity in a centralized manner.
- *Access control enforcement at the border of the mesh network:* In this case, the access control is enforced by the gateways that are placed at the border of the mesh and the wired network.
- *Distributed access control enforcement:* In this case, the access control is enforced by the access points themselves.

If the access control is enforced by a central entity or at the gateways, then the system can not benefit from authenticating the mesh clients inside the mesh network. If the access control enforcement is distributed, the mesh client can be authenticated at the following network elements:

- *Remote authentication server:* In this case, the authentication servers of the operators are placed outside of the mesh network.
- *Local authentication servers:* In this case, the authentication servers are placed near to the access points within the mesh network, therefore, they can be reached by the access points within a few wireless hops.
- *Access points as distributed authentication servers:* In a totally distributed approach, the access points themselves function as authentication servers.

During the handoff, the authentication process can be initiated in a reactive or in a proactive manner:

- *Reactive authentication:* In this case, the authentication of the mesh client to the next access point and the establishment of the connection keys are carried out when the mesh client has already associated with the next access point.
- *Proactive authentication:* In this case, the connection keys are distributed to the potential next access point before the handoff process is started.

In addition, we classify proactive solutions by the participant who controls the key distribution:

- *Mesh client driven key distribution:* Before a mesh client performs a handoff, it creates security associations with the next or with each potential next access point.
- *Authentication server driven key distribution:* An authentication server distributes mesh client specific keys among the potential next access points in such that the keys are available before the mesh client associates with the next access point.

In Table I, we categorized the proposed authentication methods found in the literature according to the above described taxonomy. In what follows, we describe the categories in more details and we outline the main idea of the related proposals.

Note that the most of the proposed authentication procedures do not take into consideration the multi-operator environment. According to this, we consider the multi-operator environment only through the formerly defined requirements and we describe them in the single operator environment unless we state otherwise.

Centralized enforcement of access control. In an architecture where the access control enforcement is centralized, no authentication is required at the access points during the handoff process. The mesh client can associate to any access point, and the access control is enforced by redirecting the traffic of the mesh client to a central access control enforcement unit. The central unit makes forwarding decisions based on the origin of the traffic, typically, based on the MAC and/or IP addresses of the mesh client. This solution is often used in WiFi hotspots, for instance, using the Chilispot implementation [6]. The main drawback is that no connection key is established and an attacker can easily gain access by spoofing the MAC and IP addresses of an already authenticated device.

Another centralized solution is proposed in [7, 8], where the authors propose an architecture based on PANA (Protocol for carrying Authentication for Network Access) [28]. The mesh client is authenticated only once, when it first associates with an access point. After a successful authentication, an IPSec tunnel can be established between the mesh client and central access control enforcement entity, which obtains the connection key from the authentication server. As only the mesh client and the access control enforcement entity can use this IPSec

DOI: 10.1002/wcm

Table I. Categorized list of the proposed authentication methods

<table>
<tr><td>Central</td><td colspan="4">[6, 7, 8, 9]</td></tr>
<tr><td>Border</td><td colspan="4">[7, 8, 9]</td></tr>
<tr><td rowspan="4">Distributed Access Control Enforcement</td><td>Key distribution type / Authenticator</td><td rowspan="2">Reactive</td><td colspan="2">Proactive</td></tr>
<tr><td></td><td>Authentication server driven</td><td>Mesh client driven</td></tr>
<tr><td>Access points</td><td>[10, 11]</td><td>[12, 13]</td><td>[14]</td></tr>
<tr><td>Local authentication servers</td><td>[15, 16]</td><td rowspan="2">[17, 18, 19]</td><td rowspan="2">[20, 21, 22, 23, 24, 25]</td></tr>
<tr><td>Remote authentication server</td><td>[20, 26, 27]</td></tr>
</table>

tunnel, this can be the basis of the access control enforcement.

The CAPWAP (Control And Provisioning of Wireless Access Points) standard [29] (currently in draft version) supports the centralized access control enforcement. The binding to the IEEE 802.11 standard is presented in [9]. Herein, the physical and link level functionality of the access points are separated and the link level functionality is implemented in a central entity. This central entity communicates with a mesh client through a tunnel established between the central entity and the access point where the mesh client is associated to. When the mesh client re-associates at a different access point, a 4-way handshake is performed between the mesh client and the central entity.

The main advantage of central access control enforcement is that no key material is stored in the access points. Hence, an attacker is not able to obtain any keys by compromising an access point. However, this architecture is extremely vulnerable to DoS attacks, because there is no possibility to deny the access before a message arrives to the central access control enforcement unit, and hence, an attacker can decrease the QoS level by injecting fake messages into the system. Another drawback is that the central unit is a bottleneck resulting in a potential scalability problem.

Access control enforcement at the gateways. When the access control is enforced at the border of the wired and the mesh network, the mesh client can authenticate either to the gateway or to a central authentication server. However, so far, no proposal exists where the gateway authenticates the mesh clients.

With the mesh networks, the operators gain a cheap or feasible way of enlargement of the wireless radio coverage. However, the main objective remains to offer access to the Internet. From this point of view, the gateways can be good points to prevent the unauthorized access as it requires less administration.

The PANA protocol proposed in [7, 8] can also be used in the case when the mesh client is authenticated to a central authentication server but the access control is enforced at the gateways. This is so because PANA allows for the existence of multiple access control enforcement entities. Hence, each gateway can be an access control enforcement entity that obtains the keys for access control enforcement from the authentication server. This mechanism improves the scalability of the centralized access control enforcement, but the DoS vulnerability described earlier still remains.

The mechanism proposed in the CAPWAP standard [9] can suit to the gateway enforced access control. In that case, the gateway is the central entity which operates some access points. However, a handover may perform between two access points which belongs to different gateways and in that case a handover between gateways should be defined.

Distributed access control enforcement with reactive authentication using a remote authentication server. A typical example of this case is the IEEE 802.1X [30] authentication and access control model as described in the IEEE 802.11i standard [20]. In this model, access control is enforced by the access points in a distributed manner. The client authenticates itself to a remote authentication server, which informs the access point about the result of the authentication, and also distributes a connection key. This connection key (or keys derived from it) is used to secure the follow-up communication at the link layer.

The messages of the authentication protocol are carried by the Extensible Authentication Protocol (EAP) [31]. While many authentication protocols have been standardized in this framework (e.g., EAP-TLS, EAP-FAST, EAP-SIM), none of them are optimized for fast handoff. Recently, a new EAP method has been described for fast re-authentication in [26] and [27].

DOI: 10.1002/wcm

We have already overviewed the CAPWAP standard [9] in distributed access control section. Recall that the physical and link level functionality of the access points are separated herein and the link level functionality is implemented in a central entity. The CAPWAP standard has a special feature (not mentioned before) which supports the delegation of the access control to the access points by sending the established connection key to the access points. The connection key is delivered due to the protocol described in the CAPWAP standard after a successful 4-way handshake performed between the mesh client and the central entity.

The main drawback of this approach is that the round trip time may increase significantly with the increasing distance (measured in wireless hops) between the access point and the authentication server. Hence, the round trip time can easily become higher than the round trip time that a QoS aware service can tolerate. Note that no application data can traverse the mesh network until the authentication is finished. Furthermore, the central authentication server is a single point of failure, which is vulnerable to DoS attacks.

Distributed access control enforcement with reactive authentication using local authentication servers. The problems listed above can be solved by using local authentication servers placed close to the access points. Two EAP standard extensions in [15, 16] are proposed to reduce the round trip time of the authentication messages by using local authentication servers placed between the access points and the central authentication server. The central authentication server is able to share the authentication key or a key derived from the authentication key with the local authentication servers. When an access point turns to any of the local authentication servers, that authentication server generates the connection key and sends it to the access point.

The main drawback of using local authentication servers is that those servers are within the mesh network where they may not be physically protected. Hence, it is hazardous to store long-term authentication information on them, as that information can be easily compromised.

Distributed access control enforcement with reactive authentication using the access points. The authentication is scalable and no preparations are required before the handoff when the authentication is performed between the mesh client and access points in a reactive way. However, other requirements may not be fulfilled as two proposals show.

The ID-based public-private key pairs can be used both for authentication and for key agreement with off-line central authority as it is exploited in [10]. However, the private keys should be issued by the same central authority. Therefore, when a mesh client associates to a foreign access point it requires to have a temporary public-private key pair from the foreign operator for the key agreement or it can obtain one after an authentication process. In the latter case, fast handoff can not be guaranteed.

In [11], the authors suggest a change in the port-based network access control operation of IEEE 802.1X. Instead of restricting the mesh client to authentication messages through the uncontrolled port, the current access point allows mesh clients access to normal data traffic via a dynamically established tunnel between the current and the previous access point. The tunnel remains alive until the authentication is completed.

Distributed access control enforcement with server driven proactive authentication. In server driven proactive authentication methods, the authentication server is responsible for distributing connection keys prior to the handoff. Thus, when the handoff is taking place, the access points are able to make access control decisions locally without turning to the authentication server.

In [17], the connection keys are generated using the authentication key, the MAC addresses of the mesh client and the access point, and the connection key used at the current access point. The authentication server generates keys for the neighbors of the current access point and distributes among them. By neighbors, we mean the potential next access points that the mesh client may associate with. In this solution, the authentication server has to be aware of the location of the mesh clients, otherwise it is not able to determine which access points need keys next. A very similar idea is described in [18] with some improvements: 1) the current AP sends the list of neighbors to the authentication server and 2) optionally, the current access point can distribute the current connection keys among the neighboring access points using IAPP protocol to postpone the connection key generation.

In [19], the GSM authentication model was adopted to a WiFi environment. The authentication server generates so called triplets which consist of some

DOI: 10.1002/wcm

authentication information and a connection key. The triplets are sent proactively to the potential next access points that can use the authentication information therein to authenticate the mesh client performing the handoff, and the connection key for further access control enforcement. As the triplets are generated by the authentication server, the access points do not have to store long-term authentication keys. No concrete triplet distribution mechanism is proposed in that paper.

Distributed access control enforcement with mesh client driven proactive authentication. In contrast to server driven proactive authentication mechanisms, in the client driven case, the mesh clients themselves are responsible for getting the connection keys to the access points.

A mechanism called pre-authentication was proposed in the IEEE 802.11i standard [20] that allows a mesh client to establish connection keys with the potential next access points prior to the handoff by performing full authentication through the current access point. The main advantage of this mechanism is that it is standardized and supports QoS aware services. However, the main drawback is that pre-authentication requires link level connection between the access points, and therefore, the mesh client can establish connection keys only with the one-hop neighbors of the current access point. Unfortunately, the set of potential next access points may not coincide the set of one-hop neighbors of the current access point.

In the IEEE 802.11r [21] standard, when a mesh client first connects to the network, it performs a full 802.1X authentication with a remote authentication server. The access point AP_0 through which this full authentication is performed will play a special role during the upcoming handovers. Before leaving the access point currently associated with, the mesh client indicates the handover and the identity of AP_0 to the next access point (through the current access point or directly). The next access point obtains an authentication key K from AP_0. The mesh client is able to generate K using some public information and the initial authentication key shared with AP_0. The handover is completed by running the 4-way handshake with the next access point and deriving connection keys from K.

The usage of multiple radio interfaces in mesh client devices was proposed in [24]. When multiple radio interfaces are available, one radio interface can be associated with a current access point and used for data traffic, while the other radio interface(s) can independently establish connection keys with other access points within radio range. The handoff then consists in swapping the roles of the radio interfaces: the radio interface which has already established a security association with the next access point becomes responsible for the data traffic, and the other radio interfaces(s) continues establishing security associations with new access points. Using multiple radio interfaces eliminates the problem that we identified in the case of pre-authentication, but this solution requires special hardware support (i.e., multiple radio interfaces) in the mesh client devices.

A solution is proposed in [22, 23] for simplifying the connection key establishment between the mesh client and all the potential next access points. For this objective, the authors modified the key distribution mechanism of the IEEE 802.1X model. According to this modification, the mesh client and the authentication server establish a new connection key through the current access point, which is then distributed by the authentication server to the potential next access points. This approach is not compatible with the IEEE 802.11i standard, and it does not satisfy the requirement of independence of connection keys, because the new connection key is distributed among all the potential next access points.

Two ticket based approaches are introduced in [25]. The idea is that after a full authentication, the authentication server generates tickets for each access point where the mesh client could move according to its mobility pattern. The tickets are delivered in one proposed solution to the potential next access points and in the other proposed solution directly to the mesh client. In the former case, the communication between the access points is based on the IEEE 802.11f protocol, also known as Inter Access Point Protocol (IAPP) [32]. In the latter case, the mesh client sends the tickets to the access point at the time of the handoff. The tickets are encrypted using unique shared secrets between each access point and the authentication server. Therefore, the access points can obtain only those keys that are related to their own connections. The main drawback of this solution is the mobility prediction mechanism that has to be very precise, otherwise, no connection key may be established at the access point which the client wants to associate with. Furthermore, the IAPP protocol was withdrawn in 2006.

Distributed access control enforcement with proactive authentication to the access point. Instead

DOI: 10.1002/wcm

of authenticating to a remote or local authentication server, in this category of solutions, the mesh client authenticates to the access point in a proactive manner.

There are two papers that follow this approach. In [14], the authors propose a solution where the currently used connection key is distributed to the potential next access points by the current access point, and it is re-used there when the handoff takes place. The drawback is that this solution does not satisfy the requirement of independence of connection keys. In addition, the access points must trust each other even if they belong to different operators, which means that the requirement of no single trusted entity is not satisfied either.

In [12, 13], the mesh client carries the new connection key in a credential that is sent to it by the current access point prior to the handoff. The credential is encrypted with a key shared between the current access point and the next access points. After associating with the next access point, the mesh client shows its credential, and the new access point decodes the connection key. Because of the time constraints, the authors propose to use symmetric cryptography to encrypt and decrypt the credentials. The authors also propose to run a full authentication after the lightweight credential based authorization. The mesh client can send data traffic parallel to the full authentication, hence, there are no constraints for the speed of the full authentication. The requirement of independence of connection keys is not fully satisfied in this solution either, because the previous access point generates the new connection keys. However, in this case, a full authentication is also carried out, therefore, this requirement remains unsatisfied only for a short period of time. The main drawback is that the mechanism as proposed does not fit any standards.

Generation of connection keys. Considering the generation of connection keys in the various proposals, the connection keys are computed using the following data (or some part of them): the authentication key, the previous connection key, public information of the access point, some random numbers. Table II shows what requirements are fulfilled by the different input data. Note that during the computation of the connection keys, these input data can be combined. However, the combination must ensure that the access points are not able to obtain the authentication key from the computed connection keys. Besides the appropriate key generation process, the independence of the connection keys can be fulfilled by performing a full authentication after the completed fast handoff.

Table II. Requirements and proposed solution for connection key generation

	Ensure freshness for the mesh client	Ensure freshness for the access point	Independence of connection keys	Long term key protection	Mutual authentication
Authentication key	✓	✗	✗	✗	✗
Previous connection key	✗	✓	✗	✓	✓
Public information of AP	✗	✓	✓	✗	✗
Random number from AS†	✗	✓	✓	✓	✗
Random number from MC	✗	✓	✓	✗	✓

† AS – Authentication server

5.3. Summary

In Table III, we summarize how the various approaches for authentication and access control enforcement described above satisfy the requirements identified earlier. Unfortunately, it is unambiguous what compatibility of a whole category with standards means.We indicate that a category is compatible with standards if at least one method found in literature is a standard or based on a standard and the standard is not in draft version. Note that the status of the compatibility can quickly change with new accepted standards or new proposed methods.

When access control is enforced at a central entity or at the border of the mesh network, the system is not able to deny the forwarding of packets coming from unauthorized mesh clients. Therefore, these methods create DoS vulnerability in the network. Furthermore, in the case of central access control enforcement, the network is not scalable, because the central access control enforcement unit becomes a bottleneck.

When a central authentication server is used with reactive authentication, the round trip time of the message exchanges of the authentication protocol can be too long such that the QoS aware services cannot tolerate that. Besides that, if the authentication server is DoS attacked, no authentication can be performed during the handoff in the entire network. These problems are solved when local authentication servers are used, but then the problem is that those servers reside in the mesh network and they can be attacked and compromised physically.

Distributed access control enforcement with proactive authentication methods satisfy all the requirements. However, not all parts of the connection key distribution process is handled in a standardized way when the key distribution process is server driven. In

DOI: 10.1002/wcm

Table III. Requirements and authentication methods

			Fast (re)authentication method	DoS resistance	Compatibility with standards	Scalability	No single trusted entity
Central access control enforcement			✓	✗	✓	✗	✓
Boundary access control enforcement			✓	✗	✓	✓	✓
Distributed ACE*	Reactive	Remote auth. server	✗	✗	✓	✗	✓
	Reactive	Local auth. server	✓	✓	✗	✓	✗
	AS driven† proactive	Authentication server‡	✓	✓	✗	✓	✓
	Mesh client driven, proactive	Authentication server‡	✓	✓	✓	✓	✓
	Reactive	Access point	✓	✓	✓	✓	✗
	AS driven† proactive	Access point	✓	✓	✗	✓	✗
	Mesh client driven, proactive	Access point	✓	✓	✗	✓	✗

* ACE – Access control enforcement
† AS – Authentication server
‡ Remote or local authentication server

the case of mesh client driven proactive authentication, the proposed mechanisms often require conditions that are difficult to satisfy (e.g., multiple radio interfaces in mesh clients).

The requirement of no single trusted entity is not satisfied when the previous access point authenticates the mesh client during or before the handoff, because an access point must trust the previous access point as an authenticator even if it belongs to another operator.

6. Protection of wireless communications

Wireless communications between mesh clients and mesh routers, as well as among mesh routers and gateways must be protected against various attacks. The main options for the protection of network communications are the following:

- *End-to-end protection:* In this case, the information is protected from the mesh client to the other endpoint of the communication, which can be located within the Internet or within the mesh network.
- *Link-by-link protection:* In this case, the information is protected only on the wireless links between the mesh routers, as well as between the mesh client and the access point. Different protection mechanisms can be applied on each link.
- *Protection of route segments:* This solution is somewhere between link-by-link and end-to-end protection. In this case, the information is protected on a segment of the route between the mesh client and the other endpoint of the communication. This can be useful if parts of the mesh network can be considered as trusted and the protection needs to be applied only in the untrusted parts.

6.1. End-to-end protection

The easiest way to implement communication security services is to use end-to-end protection solutions. End-to-end protection in this case means that the mesh client uses cryptographic methods (e.g., message authentication codes, encryption, etc.) to protect its traffic and the other endpoint, an Internet host or a target in the mesh network, checks the necessary fields and does the appropriate inverse operations.

This method has the following properties:

- It is transparent to the mesh routers, hence, there is no need to modify any mesh-internal elements.

DOI: 10.1002/wcm

- The mesh routers cannot check the integrity of the packets while they are in-transit. This means that any modified, spoofed or fabricated packet is only detectable at the endpoint, therefore, there is an elevated risk for unwanted traffic throughout the mesh network, which may lead to a DoS situation.
- End-to-end protection can cover the path within the Internet (from the gateway to the end system), not just in the mesh network. As the mesh network operator cannot protect the traffic on the Internet, only in his limited reach, the end-to-end protection is the only possibility when such coverage is needed.
- The endpoints must support the protection method and should use an up-to-date and secure implementation. This can be problematic, as the end systems are typically owned by end users.

In the case of full end-to-end protection, the network traffic between the mesh clients and the end systems (inside the mesh or in the Internet) can be protected by application level solutions, such as TLS [33] or SSH [34]. Alternatively, a network sublayer can also be introduced to provide general security services for all network traffic. For this purpose, off-the-shelf VPN (Virtual Private Network) tools are available. The most frequently used solution is an IPsec [35] connection between the endpoints.

6.2. Link-by-link protection

Link-by-link protection is the other extreme of the available approaches. It means that the information within the mesh network is protected hop-by-hop, including the link between the mesh client and the access point, and the links between the mesh routers. On every link, the operator or the two operators that share the link can decide what protection mechanisms, algorithms and keys are used, or even, what part of the traffic should be protected with such measures.

The main advantage of link-by-link protection is that the level of protection and the mechanisms used can be different on each link. Thus, depending on the properties of the link, the algorithms and parameters might be adjusted. In addition, link level protection is transparent to the endpoints, and it can also provide help against traffic analysis.

The main drawback is that the information is not protected from the mesh routers, therefore, they should be all trusted, if only link-by-link protection is used. Considering that mesh routers are physically not protected and that dishonest operators can be attackers, the assumption that all routers are trusted is not realistic. Hence, link-by-link protection should be complemented with end-to-end protection measures or route segment protection.

On the other hand, link-by-link protection is indispensable for the prevention of traffic analysis and for the avoidance of bandwidth consumption DoS attacks. In particular, link-by-link encryption can protect network meta-data, such as high level addresses and names, from disclosure to external attackers, and link-by-link integrity protection can help to detect modified or spoofed packets immediately, and therefore, it helps to avoid that modified or spoofed packets eat up network bandwidth in the mesh network. Note that when only end-to-end integrity protection is used, modified and spoofed packets are detected only at the end systems, and they can cause reduced QoS or even a DoS situation for the users.

Link level protection should be based on standard cryptographic algorithms, such as HMAC [36] for integrity protection and AES [37] for encryption. The encapsulation of the packets can use a proprietary method or it can use standardized protocols (e.g., those described in the IEEE 802.11s standard [38]), depending on the wireless networking technology used. For the protection of the link between the mesh client and the access point, standard solutions based on WPA or WPA2 [39] should be used.

An important part of the integrity protection is the protection against replays. This can be achieved by using sequence numbers and flow identifiers, and including them implicitly or explicitly in the MAC computation. In fact, such sequence numbers and flow identifiers may already be available in the packets depending on the packet format of the networking protocols used. Otherwise, the packets must be extended with additional header fields that can carry sequence numbers and flow identifiers.

6.3. Route segment protection

Between end-to-end and link-by-link protection methods, there are other scenarios where only a segment of the communication path is protected, which can be very useful in a multi-operator environment:

- *Protection only between the client and the access point:* Considering that the network operators might use directional antennas between the mesh routers, the most vulnerable

DOI: 10.1002/wcm

place against network sniffing is the wireless link between the mesh client and the access point. Therefore, this link needs special attention.

- *Protection on those parts of the mesh network that belongs to other network operators:* Depending on the trust between the mesh client and the network operator, a client may consider the operator's access points and mesh routers as secure enough. However, in a multi-operator based mesh network, it is possible that some parts of the client's traffic is handled by mesh routers that belong to other network operators. If the client's trust is lower in those operators, then it is possible to protect the traffic only in those foreign parts of the network.
- *Protection between the client and the gateway:* Beyond the gateway, the Internet may be considered as a more secure environment, as the links are generally physically protected. Therefore, the packets may only be protected within the mesh network from the mesh client up to the gateway.
- *Protection between the client and a traffic aggregation point outside of the mesh network:* One typical goal of a mesh network is to provide larger bandwidth to the customers than it would be possible with a single link. For this reason, packets belonging to a single flow may be sent through multiple gateways, and then aggregated into a single flow again at some aggregation point within the Internet. In this case, the communication between the aggregator and the mesh client can be protected based on standard protocols such as IPsec [35].

Note that route segment protection inherits some of the drawbacks of end-to-end protection. In particular, if the integrity of the packets can only be verified at the endpoints of the route segment, then modified or spoofed packets may waste valuable network resources, and thus, degrade the QoS provided to the users. In order to address this problem, one could use a broadcast authentication scheme, for instance digital signature, to ensure that the authenticity and integrity of the packets can be verified by the intermediate nodes on the route segment, while the encryption can still be used between the endpoints of the route segment. Furthermore, in order to avoid the increased overhead caused by the verification of the digital signatures, this approach can be used in a probabilistic manner, or it can be turned on only if a large number of modified or spoofed packets are detected at the endpoints of the route segment.

6.4. Protection against traffic analysis

As we said before, link-by-link encryption is an effective approach against traffic analysis, as an adversary sniffing the traffic of a wireless link is unable to distinguish between the traffic of the individual clients and cannot access traffic meta-information (e.g., IP addresses and TCP port numbers) that would reveal the identity of the service provider and the kind of service used. However, if the mesh network has a low amount of traffic, then the encrypted data may still provide useful private information for the attacker.

As an additional measure, dummy traffic might be used for the protection against traffic analysis. This means that the mesh clients and the mesh routers can continuously send dummy packets through the wireless links. The attacker cannot distinguish between dummy packets and encrypted network traffic, therefore, this solution protects against traffic analysis. A drawback of this approach is the unnecessary traffic generated and transported over the network, however, to solve this problem, the dummy traffic can be suppressed if the network links become too busy.

7. Secure routing

The problem of routing in wireless mesh networks is similar to that in mobile ad hoc networks (MANETs), as both types of network use multi-hop wireless communications. For this reason, MANET routing protocols have been considered for mesh networks both in academic and in industry circles. For instance, the IEEE 802.11s working group defined two routing protocols for 802.11 based mesh networks, and both are based on protocols proposed earlier for MANETs: the default routing protocol in the 802.11s standard is a variant of the AODV (Ad-hoc On-demand Distance Vector) protocol [40], and an optional routing protocol is also defined that is a variant of the OLSR (Optimized Link-State Routing) protocol [41]. In the remainder of this section, we assume that the reader has some basic knowledge about routing in MANETs and in mesh networks; more information on these topics can be found in [42] and [43], respectively. Our objective is to identify how mesh network routing differs from MANET routing with respect to security,

DOI: 10.1002/wcm

and to give an overview on the design options for securing mesh network routing protocols.

The main differences between MANETs and mesh networks that are relevant for routing are the following:

- The nodes in MANETs are mobile and, hence, battery powered. In mesh networks, the mesh clients can be mobile and battery powered, but the mesh routers are mainly static and they are connected to some power supply. Therefore, mesh routers are less constrained in terms of energy consumption than MANET nodes are.
- In MANETs, it is often assumed that any two nodes may want to communicate with each other. In contrast to this, mesh networks are often used as access networks through which the mesh clients connect to the Internet, meaning that the bulk of the communication is between mesh clients and gateway nodes, resulting in a more specific traffic pattern than the traffic pattern in MANETs. In addition, in mesh networks, a flow originating from a single mesh client can be split and routed towards multiple gateways, while this type of multi-destination routing is less common in MANETs.
- In MANETs, routing is best effort, and QoS issues are usually not addressed, while in mesh networks, many of the envisioned applications require QoS support from the routing protocol. Therefore, mesh network routing protocols are optimized for performance and reliability, and they use more complex routing metrics than the hop-count, which is the most commonly used metric in MANET routing protocols.

In addition to these general differences, we must also mention that MANETs are often considered to be fully self-organized, where each node is owned and administered by a different entity, while in this paper, we consider operator based mesh networks, where a group of mesh routers are owned and administered by a single entity (however, we assume the co-existence of multiple operators). This is not a general difference between MANETs and mesh networks, because MANETs can also belong to a single administrative domain (e.g., in military applications), and community based mesh networks may also be fully self-organized.

Based on the observations made above, we identify the following main differences between the security of mesh network routing and MANET routing: First of all, while the security requirements are more or less the same, in mesh network routing, QoS support mechanisms need to be protected against attacks, and in particular, the protection of routing metric values and metric computation against attacks launched by misbehaving mesh routers needs some special attention. Second, the security mechanisms can be different, in particular, in mesh networks, we can take advantage of the fact that the mesh routers have no energy constraints and can run more complex cryptographic algorithms than the nodes in MANETs. Finally, in operator based mesh networks, the establishment of security associations between the mesh routers is easier, as the necessary cryptographic material can be distributed and managed by the operators in a systematic way. For instance, the usage of public key cryptography and the assumption of a public key infrastructure run by the operators do not seem to be far fetched.

Surveys on securing MANET routing protocols can be found in [44] and in Chapter 7 of [45]; here, we focus on the differences identified above, and not covered by those surveys. More specifically, we address the protection of the routing metric values in reactive distance vector routing protocols and in proactive link-state routing protocols, as well as the security issues in resource reservation and in error recovery mechanisms. We do not address specific attacks on routing identified earlier in the literature, such as wormholes [46] and rushing [47], because those are not unique to mesh networks and they are extensively covered by the literature on MANET routing security.

7.1. Securing the route discovery

We discuss the security of the route discovery phase of two types of routing protocols: reactive distance vector routing and proactive link-state routing. Reactive distance vector routing protocols (e.g., AODV) discover routes in an on-demand manner by flooding the entire network with a route request message. Among other things, this route request message contains an aggregated routing metric value that is updated by each node that processes the message, and that represents the routing metric of the path taken by this particular copy of the message. When the nodes process a route request message, they update the routing entry that corresponds to the initiator of the route discovery by setting the routing metric value of the entry to the aggregated routing metric value observed in the request. Intermediate nodes that know a path to the destination and the destination itself can respond to a route request by sending a

DOI: 10.1002/wcm

unicast route reply message back on the reverse path taken by the request. Similar to the route request, the route reply message contains an aggregated routing metric value too that is updated by each node that processes the message. When the nodes process a route reply message, they update the routing table entry that corresponds to the destination of the route discovery by setting the routing metric of the entry to the aggregated routing metric value observed in the reply.

In proactive link-state routing protocols (e.g., OLSR), each node periodically floods the network with link-state update messages that contain the current link quality metric values observed by the node on all of its links. Based on the received link-state update messages, each node can reconstruct the connectivity graph of the network, where the edges are labeled with the link quality values. Then, each node can select the appropriate path to any other node in the network using various path selection algorithms locally.

In order to prevent the manipulation of the routing messages, and thus, the creation of incorrect routing state by an external adversary, the routing messages must be authenticated and their integrity must be protected. This can be easily achieved by using standard cryptographic techniques including digital signatures and message authentication codes (MACs). Digital signatures provide broadcast authentication services meaning that *all* nodes in the network can verify the authenticity of a signed message. For this, the public keys of the potential signers must be distributed to the verifiers securely in an off-line manner. In case of MACs, only those nodes can verify the authenticity of a message carrying a MAC value that possess the secret key used for generating that value. This requires the nodes to securely establish shared secret keys between each other. Routing messages can be protected either with a key shared by all nodes in the network or on a link-by-link basis using keys shared by neighboring nodes; both approaches prevent an external adversary from manipulating the routing messages. However, the disadvantage of relying on a common key shared by all nodes is that if a single node is compromised, then the entire system collapses. For this reason, either digital signatures should be used, or routing messages should be authenticated with MACs on a link-by-link basis using pairwise shared keys.

Reactive distance vector routing. The difficulty of securing reactive distance vector routing protocols lies in the protection against misbehaving routers. In particular, the difficulty is that the routing messages contain aggregated routing metric values that are legitimately manipulated by the nodes that process those messages. Hence, a misbehaving router can incorrectly set the aggregated routing metric value in a routing message, and there is no easy way for the other routers to detect such a misdeed. Note that authentication of routing messages does not help to solve this problem.

Recall that we are interested in QoS-aware routing for mesh networks. Here, the aggregated routing metric value of a path is computed from the link quality metric values that correspond to the links of that path. There are various link quality metrics proposed in the literature for mesh networks; most of them are based on general quality metrics such as bandwidth, delay, jitter, bit error rate, etc. However, all known link quality metrics fall in either of the following three classes: (a) *additive*, (b) *multiplicative*, and (c) *transitive* metrics. In case of additive metrics, the aggregated routing metric of a path is computed as the sum $\sum_i x_i$ of the link quality metric values x_i. Examples for such metrics are the delay, the jitter, and also the hop-count. In case of multiplicative metrics, the aggregated routing metric is computed as the product $\prod_i x_i$ of the link quality metric values. An example for such a metric is the bit error rate. Finally, in case of transitive metrics, the aggregated routing metric is either the minimum $\min_i x_i$ or the maximum $\max_i x_i$ of the link quality metric values. A transitive metric where the minimum is used is the bandwidth.

We make the observation that multiplicative metrics can be transformed into additive metrics by taking the logarithm of the metric values: $\log \prod_i x_i = \sum_i \log x_i$. Similarly, any transitive metric that uses the minimum can be converted into a transitive metric that uses the maximum by multiplying the metric values with -1: $-\min_i x_i = \max_i(-x_i)$. Therefore, it is sufficient to develop protection techniques for either additive or multiplicative metrics, and for the transitive metric that uses either the minimum or the maximum.

In addition, another observation is that routing metrics are usually monotonic, meaning that either $f(X, x) \leq X$ or $f(X, x) \geq X$ for any aggregated metric value X and any link quality metric value x, where f denotes the aggregation operator (i.e., addition, multiplication, minimum, or maximum). Clearly, the minimum and the maximum are always monotonically decreasing and increasing, respectively. Moreover, if the link quality metric values are non-negative, then additive metrics are monotonically

DOI: 10.1002/wcm

increasing, while if link quality values are non-positive, then additive metrics are monotonically decreasing. Similarly, if the link quality metric values are not smaller than one, then multiplicative metrics are monotonically increasing, while if they are not greater than one, then multiplicative metrics are monotonically decreasing.

Monotonic routing metrics can be protected against manipulation by misbehaving routers using hash chains. More specifically, hash chains can be used to protect monotonically increasing metrics against malicious decrease, and monotonically decreasing metrics against malicious increase. A detailed description of using hash chains in routing protocols can be found in [48]. The basic idea is that the routing messages contain a cryptographic hash value, and each node i that processes a routing message updates this hash value by hashing it further iteratively q_i times with a publicly known cryptographic hash function, where q_i corresponds to the link quality metric value with which the aggregated routing metric value is being increased or decreased. Thus, in order to decrease a monotonically increasing, or to increase a monotonically decreasing metric value, a misbehaving router should be able to compute pre-images of the hash value found in the routing message, and this is computationally infeasible, due to the one-way property of cryptographic hash functions.

While hash chains are efficient and easy to use, they have some limitations, the most serious one being that they can protect against either increase or decrease, but not against both. One can argue that if paths with smaller routing metric values are preferred, then it is sufficient to protect against malicious decrease of the aggregated routing metric value, while if paths with larger metric values are preferred, then it is sufficient to protect against malicious increase. Malicious modifications made in the other direction make a path less attractive, and they may result in a situation, where a given path is finally not selected when it should have been selected if there was no misbehaving router on the path. While in theory, this can be considered to be an attack, in practice, such attacks have little and uncontrolled effects, and hence, they are not very likely to happen.

The protection of the hop-count needs some special attention in case of QoS aware mesh network routing. The hop-count is a monotonically increasing metric, and thus, the hash chain approach can be used to protect it against malicious decrease. This is useful if the hop-count is used directly as a routing metric. However, the hop-count can also be used to compute the average of some link quality metrics. For this, besides the aggregated routing metric computed as the sum of the link quality metric values, routing messages must also contain the hop-count, and in order to obtain the average, the aggregated routing metric value must be divided with the hop-count value. In this case, however, the hop-count must also be protected against malicious increase, because larger hop-count values result in a smaller average value, and this increases the probability of incorrectly selecting the corresponding path. The protection of the hop-count against malicious increase is a requirement that is unique to QoS aware mesh network routing protocols that rely on the average of the link quality values, and it is not addressed by secure MANET routing protocols. Indeed, at the time of this writing, protection of the hop-count against malicious increase seems to be an open research problem.

Another problem with passing on only aggregated routing metric values in routing messages is that a router on a path cannot verify if the previous router used a correct link quality metric value to update the aggregated routing metric value in a routing message. Assuming that links are symmetric, the two end-points of a link observe the same quality metric value on that link, and if at least one of them is not misbehaving, then it can detect if the other end-point misbehaves, given that it can observe which link quality value is used by the other end-point. Hence, the possibility of making this observation must be ensured by secure distance vector routing protocols designed for mesh networks. One approach to achieve this is delaying the aggregation of link quality values: each node puts in the message (and authenticates) the link quality value that it wants to use, the next node verifies (and re-authenticates) that value, and inclusion of that value into the aggregated routing metric value happens only after this verification possibly by a third node on the path. Note that if links are not symmetric, and only one router can make a statement about the quality of a given link (in one direction), then there is no way to detect misbehaving routers.

Examples for secured reactive distance vector routing include S-AODV [49] (Secure AODV) and ARAN [50] (Authenticated Routing for Ad-hoc Networks). However, none of these protocols consider QoS-aware routing metrics. In addition, S-AODV lacks neighbor authentication, which makes it vulnerable to spoofing attacks. The detailed analysis of these protocols can be found in [51].

DOI: 10.1002/wcm

Proactive link-state routing. Proactive link-state routing protocols are much easier to secure, because the link-state update messages do not contain aggregated routing metric values, and hence, they do not need to be modified by the nodes that re-broadcast them. Instead, each node collects link quality metric values from the entire network, and aggregates them locally during the path computation. A statement about the link qualities of a node can be authenticated by the node using a broadcast authentication scheme (e.g., digital signature). In addition, those statements can be verified and countersigned by the neighbors of the node. This simplicity is intriguing and makes link-state routing protocols a preferred choice when security issues are considered.

Security extensions to the OLSR protocol based on similar ideas described above are proposed in [52]. However, that proposal lacks the verification and countersignature of the link quality statements by the neighboring nodes. Conflicting statements about a link can still be detected by the nodes, but they are unnecessarily flooded in the entire network.

7.2. Securing resource reservations

Once an available path that satisfies the required QoS requirements is discovered, reserving resources on that path is a simple matter: a resource reservation request can be sent along that path. This request must be authenticated by its originator in order to prevent an external attacker from sending spoofed reservation requests. In addition, some rate limiting mechanism should be used to limit the amount of resources that a single node can reserve in a given period of time. This is a protection measure against misbehaving nodes that try to exhaust all resources available on a path by reserving them. As requests are authenticated, such rate limiting is straightforward to implement by tracking the reservations made by a given node. Reservations can be released as a result of sending and processing explicit reservation release messages that must also be authenticated. Moreover, reservations should also be released if the reserved resources are not actually used for a certain period of time.

7.3. Design issues of error recovery mechanisms

Routing protocols usually have built-in error recovery mechanisms that can handle the situation of link breakage. However, those mechanisms are often limited to sending an error message along the remaining segments of a broken path, which informs the involved nodes that the given path is no longer functioning. Then, the usual action is that an alternative path is selected that does not contain the broken link. If no such path is available, then an entire new route discovery must be executed. This opens the door for DoS attacks, where the attacker forces the repeated execution of the route discovery algorithm, which results in a substantially increased overhead (due to flooding), and hence, increased interference and decreased QoS for a potentially large number of nodes in the network.

In order to address this problem, the error recovery mechanism should try to repair a broken path locally without the need to flood the entire network. Link-state routing protocols are advantageous again, because each node has a full view of the network graph, and hence, any node on a broken path can locally identify detours avoiding the broken link. We are not aware, however, of any specific link-state routing protocol for mesh networks that uses such a local route repair mechanism.

8. Key management

As we have seen, securing the operation of mesh networks requires the usage of cryptographic mechanisms, which rely on cryptographic keys. Key material is needed for the protection of wireless communications within the mesh network (including the communication between the mesh clients and the access points), for the protection of the routing protocol, for the protection of the messages of the mesh client authentication protocol, and potentially, for mesh client authentication itself if it is not based on simple passwords.

Given that in a multi-operator environment, security associations are often established between entities that belong to different administrative domains, a PKI based key management approach seems to be the conceptually simplest and most convenient solution here. Although, a PKI-based approach may seem to be heavy for the first sight, it may, in fact, be feasible, because here we do not require a global and general purpose PKI. We require only that the operators of the mesh network set up their own PKI, which is used only for setting up security associations between devices. Such localized solutions are routinely used today by organizations for setting up Virtual Private Networks. Also, human users need to be equipped with certificates only in the case when they are

DOI: 10.1002/wcm

authenticated using a signature based authentication method.

A PKI for multi-operator based mesh networks could be established in a rather straightforward way: Each operator runs its own Certification Authority (CA) service that issues certificates for the public keys of the mesh routers, the access points, the gateways, and the various servers (e.g., those handling mesh client authentication) operated by the given mesh network operator. Some of the operators may use public key cryptographic protocols for the authentication of their customers, in which case, the CAs of those operators issue certificates for the mesh clients' public keys too. Mesh routers, access points, gateways, servers, and mesh clients store their own certificates, and the public key of their CA. In addition, the CAs of the different operators cross-certify the public key of each other on a bilateral basis. The resulting certificates are stored in a publicly available storage, or alternatively, each mesh router, access point, gateway, and server can periodically download and locally store the certificates issued by its CA for the public keys of the other CAs.

Given such a PKI, any two entities, say A and B, can easily establish a shared key. For this, each of them can send its public key certificate to the other. A can verify B's certificate using the certificate issued by A's CA for the public key of B's CA, and the public key of A's CA. B can verify A's certificate in a similar manner. Once they have obtained each other's public key, A and B can run any public key based session key establishment protocol (see [53] for an extensive discussion of available protocols) to establish a shared secret. Moreover, any entity A can generate digital signatures, which can be verified by all other entities using the public key of A, which can be obtained and verified as described above.

Each CA can renew certificates on a regular basis depending on its own security policy. In addition, each CA can maintain a certificate revocation list (CRL) where it publishes revoked certificates. Each operator can obtain the CRL of all the other operators, and distribute all CRLs to its mesh routers, access points, gateways, and servers. Mesh clients can obtain CRLs from access points when they connect to them.

9. Intrusion detection and recovery

Intrusion detection involves the automated identification of unusual activity by collecting audit data, and comparing it with reference data. A primary assumption of intrusion detection is that a network's normal behavior is distinct from abnormal or intrusive behavior. Various approaches to intrusion detection differ in the features (or measures/metrics) they consider, in addition to how and where these features are measured. Identifying the features to be monitored is important, because the amount of monitored data can be particularly large, and its collection can consume a significant amount of wireless resources.

Intrusion detection procedures can be classified into three categories [54]: misuse (or signature-based) detection, anomaly detection, and protocol-based (or specification-based) detection. The three categories differ in the reference data that is used for detecting unusual activity: misuse detection considers signatures of unusual activity, anomaly detection considers a profile of normal behavior, and specification-based detection considers a set of constraints characterizing the normal behavior of a specific protocol or program.

Intrusion detection in wireless mesh networks imposes additional challenges compared to intrusion detection in wired networks, due to variations and impairments of the wireless channel, the broadcast and open access nature of the wireless spectrum, the interference between wireless links, and the limited physical protection of the network nodes. For example, in an operator's wired network it is sufficient to implement intrusion detection in the edge switches or routers, which connect to external devices, and physically protect internal network devices. On the other hand, in wireless mesh network the previous differentiation of internal and edge devices is useless, since all mesh nodes, including those without links to external devices, can be affected by external sources due to the broadcast nature of the wireless spectrum.

Intrusions into wireless networks often aim at Denial-of-Service at different layers including the physical, MAC, and network layers [55]:

- *Physical layer:* The simplest form of a physical layer attack is a continuous jammer, which generates a continuous high power signal across the entire channel bandwidth. Another possibility is to transmit a periodic or random signal [56, 57].
- *MAC layer:* Attacks in this layer are referred to as *virtual jamming*, and involve transmitting spurious or modified MAC layer control (RTS, CTS, ACK) or data packets. Virtual jamming attacks can also be conducted by manipulating the NAV (Network Allocation Vector) value of control and data packets, thus influencing a well-behaving node's backoff.

DOI: 10.1002/wcm

Such actions can be performed in a continuous, periodic or random, or intelligent (channel and protocol-aware) manner [58, 56, 57, 59]. Intelligent attacks utilize the semantics of data transmission, and have the advantage of using less energy compared to continuous jamming attacks.

- *Network layer:* Attacks in this layer involve sending spurious routing messages, modified routing information, or tampering with packet forwarding.

Note that attacks can be performed in multiple layers or from multiple locations simultaneously, making them stealthy hence harder to detect. In addition, attacks can also target the transport layer and higher, however, such attacks can be handled in a manner similar to wired networks.

9.1. Related work

A distributed and cooperative architecture for anomaly detection is presented in [60, 61]. This work relies on characterizing normal behavior using an information-theoretic metric: entropy and conditional entropy. The anomaly detection approach is evaluated for identifying routing attacks, and considers multiple features that correspond to manipulating routing information and influencing the packet forwarding behavior.

The work in [62] considers the combination of multiple features, such as route additions, removals, repairs, and traffic related features such as packet inter-arrivals, to detect routing attacks. The work in [63] considers the route lifetime and frequency of routing events to detect abnormal behavior.

The work in [64] detects MAC-layer misbehavior based on the sequential probability ratio test, which is applied to the time series of backoff times; the latter are estimated using timestamps of RTS/CTS and acknowledgement packets. MAC-layer misbehavior detection is also the focus of [65], which considers a protocol-based approach that relies on detecting deviations of the values of MAC-layer parameters, such as inter-frame spacing, NAV, and backoff.

Prior work has shown the need for cross-layer and cross-feature intrusion detection. In particular, [56] shows that single metrics, such as the signal strength, packet delivery ratio, or channel access time, alone are not able to effectively detect wireless jamming. On the other hand, combining packet delivery ratio measurements with signal strength measurements or location information can detect attacks ranging from continuous physical layer jamming up to reactive jamming where the attacker transmits a jamming signal only when he detects the existence of a legitimate transmission. The work in [66] considers the combination of measurements such as the physical carrier sense time, the rate of RTS/CTS transmissions, the channel idle period, and the number of transmissions together with the channel utilization time to demonstrate that the combination of such cross-layer metrics can improve detection. Both the above two approaches consider simple threshold schemes for signaling a potential attack.

9.2. Unique features of wireless mesh networks

Wireless mesh networks have some common characteristics with wireless ad hoc networks, namely routing and forwarding over wireless multi-hop paths, hence approaches for intrusion detection in wireless ad hoc networks are relevant. Nevertheless, there are important differences, which affect both the procedures for intrusion detection and the actions for recovery.

Fixed mesh nodes and relatively stable topology. Unlike ad hoc networks, where nodes are typically mobile, in wireless mesh networks nodes are typically stationary. This has two implications: First, location information can be used for intrusion detection. Second, unlike ad hoc networks, wireless mesh networks have a relatively stable topology, which changes in the case of node failures or additions, interference, and security attacks. The reduced variability due to the stable topology yields less overhead for statistical anomaly detection approaches that require (re-)estimating the normal behavior when the network topology changes. Moreover, fixed mesh nodes typically contain higher processing and storage capabilities and have an available power supply, thus reducing the burden for estimating the normal traffic behavior compared to resource (processing, storage, and battery) constrained mobile devices.

Interconnection to a wired infrastructure and centralized management. Ad hoc networks have a dynamically varying topology with no fixed infrastructure and no centralized control. On the other hand, wireless mesh networks have a number of gateways connected to a wired network infrastructure; the existence of multiple gateways provides higher protection to intrusion attacks. Moreover, operator-owned mesh networks have centralized management.

DOI: 10.1002/wcm

Centralized management facilitates the collection of intrusion detection data and results, thus enabling correlation of measurements from different monitoring locations. Nevertheless, centralized collection and processing of all audit data may be too costly due to the consumption of scarce wireless resources.

Multi-radio, multi-channel, and directional antennas. Ad hoc networks, due to the mobility of nodes, typically involve nodes with a single radio connected to an omnidirectional antenna; moreover, to achieve connectivity all nodes operate on the same channel. On the other hand, wireless mesh networks involve nodes with multiple radios, each operating in different channels. Multi-radio and multi-channel operation results in less variability, since it reduces – but does not eliminate – the interference between links that involve different wireless interfaces. Reduction of such interference is also achieved with the use of directional antennas, which is typical in metropolitan wireless mesh network deployments. As indicated above, less variability facilitates the application of anomaly detection which uses statistical techniques for estimating normal mesh network behavior. Directional antennas also provide more resistance to jamming, since they reduce the possible positions of an attackers transmitter that can disturb the wireless communication. Moreover, multi-radio and multi-channel operation, together with directional antennas can support multiple paths between mesh nodes that contain disjoint links; availability of such multiple paths can facilitate attack recovery and mitigation, as further discussed in Section 9.4.

9.3. Requirements for intrusion detection

Based on the above discussion, next we identify requirements for intrusion detection in wireless mesh networks. At a high level, these requirements are similar to other environments such as wired and ad hoc networks. Our goal here is to discuss the realization of the requirements in wireless mesh networks.

- *Cross-feature and cross-layer detection:* Combining multiple features and measurements (cross-feature) and measurements at different layers (cross-layer) can improve the performance of intrusion detection systems. In particular, for anomaly detection such an approach can significantly reduce the number of false positives [56, 66]. Combining multiple features for intrusion detection can be achieved through a hierarchical or cascaded system: A hierarchical system recursively combines or fuses multiple alerts, i.e., deviations of individual features; such an approach can reduce the number of false positives. In a cascaded intrusion detection system, an alert for one feature can trigger a detector for another feature; in addition to reducing the number of false positives, such an approach also reduces the overhead of intrusion detection.
  Possible features (or measures/metrics) at various layers that can be used for intrusion detection include the following:
  - *Physical layer:* signal strength, packet delivery ratio (or packet error ratio), physical carrier sensing time, location information.
  - *MAC layer:* channel access delay, backoff time, channel idle time, RTS/CTS transmission rate, channel utilization.
  - *Network layer:* route update frequency (or route lifetime), route update message rate, route length. These metrics can be monitored for each mesh node that participates in routing.
  - *Application layer:* throughput, goodput, delay, jitter.
- *Distributed intrusion detection with correlation of measurements from multiple locations:* Correlation of measurements or detection results from multiple locations exploits the broadcast nature of wireless transmissions, whereby the transmission from one node can be received by multiple nodes within its range. Combining measurements from multiple monitoring locations can improve the performance of intrusion detection, by reducing the number of false positives, but requires a central entity to collect and combine the measurements from multiple locations. This suggests a two-layer intrusion detection system, where processing based on purely local information is performed in the mesh nodes, and the correlation of detection results from different monitoring locations is performed in some centralized entity. Moreover, the above can involve multiple monitors from different operators.

In addition to the above, general requirements include effective intrusion detection, in terms of high detection probability, and low false positives and false negatives,

DOI: 10.1002/wcm

and low overhead for collecting and processing monitoring data.

9.4. Attack recovery and mitigation

Here, we identify the actions and the corresponding mechanisms that can be used for attack recovery and mitigation, which are triggered by intrusion detection.

- *Channel switching:* One approach for evading an attack is channel switching (or channel hopping) [67, 68, 69]. This approach is motivated by frequency hopping, but differs in that channel switching occurs on-demand, rather than in a predefined or pseudo-random manner, thus forcing an intruder to jam a much larger frequency band. Aside selecting the new channel to switch to, channel switching requires coordination between interfaces operating in the same channel. This coordination issue is different in single-radio wireless mesh networks, compared to multi-radio mesh networks, where each mesh node contains multiple radio interfaces operating in different channels.
- *Power and rate control:* Increasing the transmission power or reducing the transmission rate can increase the energy per bit that reaches the receiver, which, in turn, increases the probability of successful packet decoding. With the former approach, when increasing the transmission power, care must be taken, as it can also increase the level of interference induced on other receiving interfaces.
- *Mechanism-hopping:* The work of [70] proposes a mechanism-hopping approach which can be viewed as a generalization and combination of channel hopping, and power and rate control, that exploits multiple mechanisms and parameters for each mechanism in all layers. For example, the physical layer includes power control and rate control/modulation, the link layer includes different medium access mechanisms with different parameters, the network layer includes different routing algorithms and forwarding strategies, etc.
- *Multi-path routing:* While channel hopping exploits channel/frequency diversity, the existence of multiple paths between mesh nodes enables space diversity. Multiple paths can be used to reroute traffic when an intrusion is detected. With this approach, the detection delay and the rerouting delay determines the impact of an attack in terms of lost data. Moreover, multiple paths can be used to perform path hopping, where a path for a particular node pair or flow is randomly switched among multiple available paths. In response to an attack, routing can be used to isolate some portion of the mesh network that has been the target of an attack. An alternative approach that can avoid data loss altogether is to combine multi-path redundancy with network coding. Intrusion detection and recovery in this context has the objective of increasing the redundancy of the mesh network in order to combat future attacks.
- *Multiple wired Internet gateways:* Another form of space diversity is the existence of multiple gateways that connect the wireless mesh network to a wired network infrastructure. The existence of multiple coordinating gateways, through the use of anycasting, can help mitigate intrusion attacks.

Note that the above actions and mechanisms pertain to the physical, link, and network layers which are specific to wireless mesh networks. These can be combined with higher layer mechanisms, such as filtering, rate limiting, and caching, to further enhance the effectiveness of attack recovery and mitigation.

10. Conclusion and future work

In this paper, we addressed the problem of securing QoS-aware mesh networks operated by multiple mesh network operators. This is a complex problem domain, therefore, our main objective was to structure it, and to give an overview of the possible design options for a comprehensive security architecture for such networks. For this purpose, we identified an attacker model and, based on that, we derived the main security requirements. Then, we gave a detailed overview on the state-of-the-art in client authentication and access control in wireless networks, and we evaluated how the various approaches proposed so far fit the requirements identified for mesh networks. Next, we identified several approaches to protect the communication within the mesh network based on standard communication security mechanisms. We also identified possible approaches to secure the routing protocols in mesh networks, and in particular to protect the routing metric values in routing messages. Finally, we identified possible approaches for intrusion and misbehavior detection and recovery that take into account the unique features of mesh

DOI: 10.1002/wcm

networks, and we proposed a PKI-based approach to key management.

We saw that, although, a considerable amount of related work has already been carried out for securing WiFi networks and mobile ad hoc networks, the results of those works cannot always be directly used in mesh networks. In particular, the authentication mechanisms available for WiFi networks do not really support user mobility, as they do not allow for seamless handover between access points, and the majority of the secure routing protocols proposed for mobile ad hoc networks do not support the protection of QoS-aware routing metrics. In addition, intrusion and misbehavior detection and recovery mechanisms proposed for wired networks and for mobile ad hoc networks are not optimized for mesh networks; they should be adapted to the characteristics of mesh networks to increase their performance in terms of effectiveness and reliability.

In terms of future work, we intend to design and implement a comprehensive security architecture for multi-operator based QoS aware wireless mesh networks that satisfies the requirements identified in this paper and takes into consideration the design choices that have been reviewed here.

Acknowledgement

This work was supported in part by the European Commission in the context of the 7th Framework Programme through the EU-MESH Project (Enhanced, Ubiquitous, and Dependable Broadband Access using MESH Networks, ICT-215320, www.eu-mesh.eu) and in part by the Mobile Innovation Center (www.mik.bme.hu) at the Budapest University of Technology and Economics.

References

1. Akyildiz IF, Wang X, Wang W. Wireless mesh networks: a survey. *Computer Networks* March 2005; **47**(4):445–487.
2. Bruno R, Conti M, Gregori E. Mesh networks: commodity multihop ad hoc networks. *IEEE Communications Magazine* 2005; **43**(3):123–131.
3. Zhang W, Wang Z, Das SK, Hassan M. Security issues in wireless mesh networks. *Wireless Mesh Networks: Architectures and Protocols*, Hossain E, Leung KK (eds.), Springer, 2008.
4. Ben Salem N, Hubaux JP. Securing wireless mesh networks. *IEEE Wireless Communications* April 2006; .
5. Falk R, Huang CT, Kohlmayer F, Sui AF. Security in wireless mesh networks. *Wireless Mesh Networking: Architectures, Protocols and Standards*, Zhang Y, Luo J, Hu H (eds.), Auerbach Publications, Taylor & Francis Group, 2006.
6. ChilliSpot - Open Source Wireless LAN Access Point Controller. `http://www.chillispot.info/`.
7. Cheikhrouhou O, Laurent-Maknavicius M, Chaouchi H. Security architecture in a multi-hop mesh network. *In Proc. 5th Conference on Security and Network Architectures (SAR 2006)*, 2006.
8. Khan K, Akbar M. Authentication in Multi-Hop Wireless Mesh Networks. *World Academy Of Science, Engineering And Technology* 2006; :178–183.
9. Calhoun P, Montemurro M, Stanley D. CAPWAP Protocol Binding for IEEE 802.11 October 2008. (work in progress).
10. Zhang Y, Fang Y. A secure authentication and billing architecture for wireless mesh networks. *Wireless Networks* 2007; **13**(5):663–678, doi:http://dx.doi.org/10.1007/s11276-006-8148-z.
11. Chen JJ, Tseng YC, Lee HW. A Seamless Handoff Mechanism for IEEE 802.11 WLANs Supporting IEEE 802.11i Security Enhancements. *IEEE Asia-Pacific Wireless Communications Symposium*, Hsinchu, Taiwan, 2007.
12. Chen T, Schäfer G, Fan C, Adams S, Sortais M, Wolisz A. Denial of service protection for optimized and qos-aware handover based on localized cookies. *Proc. of European Wireless 2004*, Barcelona, Spain, 2004.
13. Aura T, Roe M. Reducing Reauthentication Delay in Wireless Networks. *SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, IEEE Computer Society: Athens, Greece, 2005; 139–148, doi: http://dx.doi.org/10.1109/SECURECOMM.2005.58.
14. Mishra A, ho Shin M, Arbaugh WA. Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network. *INFOCOM*, IEEE, 2004.
15. Narayanan V, Dondeti L. EAP Extensions for EAP Re-authentication Protocol (ERP). RFC 5296 (Proposed Standard) Aug 2008. URL `http://www.ietf.org/rfc/rfc5296.txt`.
16. Lopez RM, Skarmeta AG, Bournelle J, Laurent-Maknavicus M, Combes JM. Improved EAP keying framework for a secure mobility access service. *IWCMC '06: Proceedings of the 2006 international conference on Wireless communications and mobile computing*, ACM: New York, NY, USA, 2006; 183–188, doi:http://doi.acm.org/10.1145/1143549.1143587.
17. Mishra A, Shin MH, Petroni J NL, Clancy T, Arbaugh W. Proactive key distribution using neighbor graphs. *Wireless Communications, IEEE [see also IEEE Personal Communications]* Feb 2004; **11**(1):26–36, doi: 10.1109/MWC.2004.1269714.
18. Kassab M, Belghith A, Bonnin JM, Sassi S. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks. *WMuNeP '05: Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling*, ACM: New York, NY, USA, 2005; 46–53, doi:http://doi.acm.org/10.1145/1089737.1089746.
19. Bohák A, Buttyán L, Dóra L. An User Authentication Scheme for Fast Handover Between WiFi Access Points. *In Proceedings of the Third Annual International Wireless Internet Conference*, ACM: Austin, Texas, USA, 2007.
20. IEEE Std 80211i^{TM}. Medium Access Control (MAC) security enhancements, amendment 6 to IEEE Standard for local and metropolitan area networks part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications. July 2004.
21. IEEE 80211r^{TM}-2008. IEEE 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 2: Fast BSS Transition July 2008.
22. Pack S, Choi Y. Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model. *PWC '02:*

Proceedings of the IFIP TC6/WG6.8 Working Conference on Personal Wireless Communications, Kluwer, B.V.: Deventer, The Netherlands, The Netherlands, 2002; 175–182.
23. Pack S, Choi Y. Fast handoff scheme based on mobility prediction in public wireless LAN systems. *IEE Proceedings Communications*, vol. 151, IEEE, 2004; 489–495.
24. Brik V, Mishra A, Banerjee S. Eliminating handoff latencies in 802.11 WLANs using multiple radios: applications, experience, and evaluation. *IMC'05: Proceedings of the Internet Measurement Conference 2005 on Internet Measurement Conference*, USENIX Association: Berkeley, CA, USA, 2005; 27–27.
25. Aboudagga N, Eltoweissy M, Quisquater JJ. Fast Roaming Authentication in Wireless LANs. *2nd International Computer Engineering Conference: Engineering the Information Society*, Cairo, Egypt, 2006.
26. Maccari L, Fantacci R, Pecorella T, Frosali F. A secure and performant token-based authentication for infrastructure and mesh 802.1x networks. *In Proceedings of the IEEE International Conference on Communications 2006*, IEEE, 2006.
27. Maccari L, Fantacci R, Pecorella T, Frosali F. Secure, fast handhoff techniques for 802.1X based wireless network. *In Proceedings of the IEEE International Conference on Communications 2006*, IEEE, 2006.
28. Forsberg D, Ohba Y, Patil B, Tschofenig H, Yegin A. Protocol for Carrying Authentication for Network Access (PANA). RFC 5191 (Proposed Standard) May 2008. URL `http://www.ietf.org/rfc/rfc5191.txt`.
29. Calhoun P, Montemurro M, Stanley D. CAPWAP Protocol Specification October 2008. (work in progress).
30. IEEE Std 8021X-2001. IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control June 2001.
31. Aboba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H. Extensible Authentication Protocol (EAP). RFC 3748 (Proposed Standard) Jun 2004. URL `http://www.ietf.org/rfc/rfc3748.txt`, updated by RFC 5247.
32. IEEE Std 80211f™. IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation July 2003. (withdrawal in 2006).
33. Dierks T, Allen C. The tls protocol 1999. RFC 2246.
34. Ylonen T, C Lonvick E. The secure shell (ssh) protocol architecture 2006. RFC 4251.
35. Kent S, Seo K. Security architecture for the internet protocol 2005. RFC 4301.
36. Krawczyk BM H, Canetti R. Hmac: Keyed-hashing for message authentication 1997. RFC 2104.
37. FIPS 197. Advanced Encryption Standard. Federal Information Processing Standards Publication 197, US Department of Commerce, Bureau of Standards, National Technical Information Service (NIST) 2001.
38. IEEE 80211s™/D20. IEEE 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. Draft amendment to standard IEEE 802.11™: ESS Mesh Networking March 2008. (work in progress).
39. IEEE Std 80211™-2007. Revision of IEEE Std 802.11-1999: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications June 2007.
40. Perkins C, Belding-Royer E, Das S. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental) Jul 2003. URL `http://www.ietf.org/rfc/rfc3561.txt`.
41. Clausen T, Jacquet P. Optimized Link State Routing Protocol (OLSR). RFC 3626 (Experimental) Oct 2003. URL `http://www.ietf.org/rfc/rfc3626.txt`.
42. Royer EM, Toh C. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications* April 1999; **6**(2):46–55.
43. Bahr M, Wang J, Jia X. Routing in wireless mesh networks. *Wireless Mesh Networking: Architectures, Protocols and Standards*, Zhang Y, Luo J, Hu H (eds.), Auerbach, 2006.
44. Hu YC, Perrig A. A survey of secure wireless ad hoc routing. *IEEE Security and Privacy Magazine* May/June 2004; **2**(3):28–39.
45. Buttyán L, Hubaux JP. *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2008.
46. Hu Y, Perrig A, Johnson D. Packet leashes: a defense against wormhole attacks in wireless networks. *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, San Francisco, CA, USA, 2003.
47. Hu YC, Perrig A, Johnson D. Rushing attacks and defense in wireless ad hoc network routing protocols. *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, San Diego, CA, USA, 2003.
48. Hu Y, Perrig A, Johnson D. Efficient security mechanisms for routing protocols. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA, 2003.
49. Zapata MG, Asokan N. Securing ad hoc routing protocols. *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, Atlanta, GA, USA, 2002.
50. Sanzgiri K, Dahill B, Levine B, Shields C, Belding-Royer E. A secure routing protocol for ad hoc networks. *Proceedings of the International Conference on Network Protocols (ICNP)*, Paris, France, 2002.
51. Ács G, Buttyán L, Vajda I. Provable security of on-demand distance vector routing in wireless ad hoc networks. *Proceedings of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, Visegrad, Hungary, 2005.
52. Raffo D, Adjih C, Clausen T, Muhlethaler P. An advanced signature system for OLSR. *Proceedings of the ACM Workshop on Security of Ad hoc and Sensor Networks (SASN)*, 2004.
53. Boyd C, Mathuria A. *Protocols for Authentication and Key Establishment*. Springer, 2003.
54. Mishra A, Nadkarni K, Patcha A. Intrusion Detection in Wireless Ad Hoc Networks. *IEEE Wireless Communications* February 2004; :48–60.
55. Wood A, Stankovic J. Denial of Service in Sensor Networks. *IEEE Computer* 2002; **35**:53–57.
56. Xu W, Trappe W, Zhang Y, Wood T. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. *Proc. of ACM MobiHoc*, 2005.
57. Thuente D, Acharya M. Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks. *Proc. of IEEE MILCOM*, 2006.
58. Gupta V, Krishnamurthy S, Faloutsos M. Denial of service attacks at the MAC layer in wireless ad hoc networks. *Proc. of IEEE MILCOM*, 2002.
59. Bayraktaroglu E, King C, Liu X, Noubir G, Rajaraman R, Thapa B. On the Performance of IEEE 802.11 under Jamming. *Proc. of IEEE INFOCOM*, 2008.
60. Zhang Y, Lee W. Intrusion Detection in Wireless Ad-Hoc Networks. *Proc. of ACM MobiCom*, 2000.
61. Zhang Y, Lee W, Huang YA. Intrusion Detection Techniques for Mobile Wireless Networks. *Wireless Networks* September 2003; **9**(5):545–556.
62. Huang YA, Fan W, Lee W, Yu P. Cross-feature analysis for detecting ad-hoc routing anomalies. *Proc. of 23rd Intl Conference on Distributed Computing Systems*, 2003.

DOI: 10.1002/wcm

63. Liu H, Gupta R. Temporal Analysis of Routing Activity for Anomaly Detection in Ad hoc Networks. *IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, 2006.
64. Radosavac S, Moustakides G, Baras J, Koutsopoulos I. An analytic framework for modeling and detecting access layer misbehavior in wireless networks. *ACM Transactions on Information and System Security* November 2008; **11**(4).
65. Raya M, Aad I, Hubaux JP, Fawal AE. DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots. *IEEE Transactions on Mobile Computing* 2006; **5**(12).
66. ans S Mishra GT, Sridhar R. A Cross-layer Approach to Detect Jamming Attacks in Wireless Ad Hoc Networks. *Proc. of IEEE MILCOM*, 2006.
67. Xu W, Wood T, Trappe W, Zhang Y. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. *Proc. of ACM Workshop on Wireless Security (WiSe)*, 2004.
68. Xu W, Ma K, Trappe W, Zhang Y. Jamming Sensor Networks: Attack and Defense Strategies. *IEEE Network* May/June 2006; :41–47.
69. Navda V, Bohra A, Ganguly S, Rubenstein D. Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks. *Proc. of IEEE INFOCOM*, 2007.
70. Liu X, Noubir G, Sundaram R, Tan S. SPREAD: Foiling Smart Jammers using Multi-layer Agility. *Proc. of IEEE INFOCOM*, 2007.

DOI: 10.1002/wcm