Journal of Network and Computer Applications ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Security analysis of wireless mesh backhauls for mobile networks

Frank A. Zdarsky [a,*], Sebastian Robitzsch [b], Albert Banchs [c]

[a] NEC Network Laboratories, Kurfürsten-Anlage 36, 69115 Heidelberg, Germany
[b] University College Dublin, Performance Engineering Laboratory, Belfield, Dublin 4, Ireland
[c] Universidad Carlos III de Madrid, Dept. of Telematics Eng., Avda de la Universidad, 30, 28911 Leganés, Madrid, Spain

ARTICLE INFO

Article history:
Received 15 October 2009
Received in revised form
30 January 2010
Accepted 25 March 2010

Keywords:
Security analysis
Wireless mesh backhauls
Mobile networks

ABSTRACT

Radio links are used to provide backhaul connectivity for base stations of mobile networks, in cases in which cable-based alternatives are not available and cannot be deployed in an economic or timely manner. While such wireless backhauls have been predominantly used in redundant tree and ring topologies in the past, mobile network operators have become increasingly interested in meshed topologies for carrier-grade wireless backhauls. However, wireless mesh backhauls are potentially more susceptible to security vulnerabilities, given that radio links are more exposed to tampering and given their higher system complexity.

This article extends prior security threat analyses of 3rd generation mobile network architectures for the case of wireless mesh backhauls. It presents a description of the security model for the considered architecture and provides a list of the basic assumptions, security objectives, assets to be protected and actors of the analysis. On this foundation, potential security threats are analyzed and discussed and then assessed for their corresponding risk. The result of this risk assessment is then used to define a set of security requirements. Finally, we give some recommendations for wireless mesh backhaul designs and implementations following these requirements.

1. Introduction

Radio links are used to provide backhaul connectivity for base stations of mobile networks, in cases in which cable-based alternatives are not available and cannot be deployed in an economic or timely manner. To ensure high availability, such wireless backhauls have been predominantly used in redundant tree and ring topologies. Yet, following the success of WiFi-based wireless mesh networks in recent years, mobile network operators have become increasingly interested in meshed topologies for carrier-grade wireless backhauls as well.[1] Mesh topologies may provide availability levels comparable to redundant trees and rings, while being more flexible and using capacity more efficiently.

However, radio links are also more exposed, and thus easier to tap and to interfere with, than their wired counterparts. This makes wireless backhauls, and in particular multi-hop ones like in wireless meshes, potentially more susceptible to security vulnerabilities. For carrier-grade wireless mesh backhaul solutions security therefore becomes a high priority non-functional requirement.

Mobile network operators have high security demands in order to protect their business assets. Assets not only include the mobile network infrastructure and services, which must be protected from unauthorized use and from attacks on their availability or quality, but an important asset requiring protection is furthermore an operator's reputation with current and potential customers. They thus need to ensure that their customers' data that is transported via their networks is protected against misappropriation. In some legislation, this is even an obligation of carriers as part of their due diligence.

Architectural design issues can quickly compromise these security goals. A prominent example is GSM's security architecture that only requires user authentication towards the network. In contrast, the network itself is not authenticated to its users. This design flaw has subsequently been exploited to mount "false base station attacks": An attacker uses a device popularly called "IMSI-catcher", which pretends to be a legal base station with a superior signal quality. This causes mobile phones in the vicinity to associate themselves with the false base station, which then signals the mobile phones to switch off encryption, as investigated by Adoba et al. (2004). Similar attacks have been reported for Universal Mobile Telecommunication System (UMTS) networks by exploiting Global System for Mobile Communications (GSM) backward compatibility, as stated in Adoba et al. (2008).

* Corresponding author. Tel.: +49 6221 4342 142.
E-mail addresses: Frank.Zdarsky@neclab.eu (F.A. Zdarsky), Sebastian.Robitzsch@ucdconnect.ie (S. Robitzsch), banchs@it.uc3m.es (A. Banchs).

[1] The EU project CARMEN (2008) is designing a wireless mesh network architecture capable of supporting carrier-grade requirements over a diverse set of radio technologies.

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.03.029

Although security attacks are well studied in 3G networks (the reader is referred e.g. to (*iGillott* Research, 2007) for a study of security in 3G networks including some statistics on attacks in the past), the multihop nature of Wireless Mesh Backhauls (WMBs) exposes the network to new security threats which require additional measures to counteract. This article therefore extends the security threat analysis of 3G network architectures by 3GPP (2001) for the case of WMBs.

The following section provides an overview of related work. Section 3 starts with a description of the security model for the considered architecture. It then provides a list of the basic assumptions made for the subsequent security analysis and introduces the security objectives, the assets to be protected and the actors of this analysis. On this foundation, potential security threats are analyzed and discussed in Section 4. They are classified both by the security objective under attack and the point of attack. Not all identified security threats are equally likely, as they require various levels of sophistication of an attacker. Also, the impact of a successful attack on the mobile network operator can vary. Thus, Section 5 performs a risk assessment of the identified security threats. The result of this risk assessment is then used to define a set of security requirements for wireless mesh backhauls. These requirements are outlined in Section 5.5. Section 6 then provides a list of general recommendations to meet these requirements for the design of wireless mesh backhaul architectures and protocols. Finally, Section 7 provides a short summary of the findings in this analysis.

2. Related work

Over the last years, a number of security architectures and mechanisms have been devised for Wireless Mesh Networks (WMNs).

Some of these works address user authentication in WMNs. For example, Zhang and Fang (2006) propose ARSA, a security architecture that allows users to access and roam between a multitude of WMNs belonging to different administrative domains based on a "pass" of a third-party provider. This is supposed to resolve the problem of establishing pair-wise trust relationships between the operators of the different WMNs. They also address the problem of user location privacy by providing the user with different alias identities. Similarly, Ren et al. (2010) describe PEACE, a security solution with authentication and key agreement protocols that provide protection against attacks on user privacy while providing a strict user access control.

Other papers address Denial of Service (DoS) attacks in WMNs. For example, Yan et al. (2009) study DoS attacks in which attackers generate a flood of high-rate data flows to deny service to other, legitimate traffic. They use a frequency analysis of incoming packets to detect such attacks and study different strategies of countering these attacks through selective random dropping.

Yet other papers address attacks on the control plane protocols of WMNs. For example, Naveed and Kanhere (2006) study attacks on dynamic channel assignment in 802.11-based WMNs, in which a compromised mesh node manipulates control messages of the channel assignment protocol to force mesh links to use heavily congested channels. Similarly, a number of attacks on routing protocols in WMNs and ad-hoc networks exist (see Hu and Perrig, 2004 for a survey of such attacks).

All of these works aim at addressing some security threats that according to the authors' intuition is relevant for WMNs. However, none of them contains a systematic approach to determine which security threats are really relevant and should require more efforts to prevent them. This question is particularly relevant if a wireless mesh network is used as backhaul for a mobile cellular network. In this case, many security features are already provided by the mobile network, for example the authentication framework with pair-wise trust relationships between operators, the handling of temporal identities and the policing of user data flows. Furthermore, all network entities are under a single administrative control, which facilitates protection of the control and data planes. In contrast to all these previous works, in this paper we conduct a complete analysis of security threats with focus on WMBs for mobile networks.

3. System model and security model

As stated in the introduction, before describing the potential security threats of a WMB a detailed system description is necessary to provide a reasonable understanding of the considered network architecture. Hence, this section presents the system model, the assumptions, the security objectives, the assets and the actors considered in the following threat analysis.

3.1. System description

Prior to going into the detailed analysis of the potential security issues, it is necessary to clearly delimit the system under test. When doing so, it is important to consider that a wireless mesh backhaul is supposed to provide a drop-in replacement for parts of the operator's wired backhaul. As such, it represents only a small sub-system within a complete mobile network architecture, e.g. a 3rd Generation Partnership Project (3GPP) architecture. It is valid to assume that this architecture provides its own security features, designed based on a separate security analysis. In case of 3GPP, the security analysis is documented in 3GPP (2001).

Fig. 1 shows the system security model of a traditional wireless access network with wired backhaul. It focuses on the transport stratum, i.e. all protocols required for the provisioning of a data transport between a user terminal (UT) and the core network. It further distinguishes between the management and control plane and the data plane of this stratum. The former divides into the user signaling part between the UT and its Point of Attachment (PoA) to the network, which in a mobile network is a wireless link, and the core network signaling part between the network elements of the access network and the core network, which is typically wired, but may use non-meshed wireless links for backhaul. The data plane transports data between the UT and the core network. This data traffic is typically end-to-end[2] encrypted. Note that the data plane from the point of view of the transport stratum may also carry management and control messages of the next higher stratum, i.e. the serving/home network stratum.

User signaling, core network signaling and user data form three "security domains", in the sense that if an attacker succeeds in overcoming the security features of one domain, all subsystems within this domain are compromised, but not necessarily those of other domains. The latter depends on how well domains are "firewalled" from each other. Fig. 2 shows the security domains of an access network using a WMB for backhaul. The figure also shows the security domains of the traditional access as grayed-out arrows, which are not covered in the present analysis, as it is assumed that proper security features to protect them are

[2] End-to-end in the sense of all the way between UT and the core network, so the content of data is not visible to the access network.

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

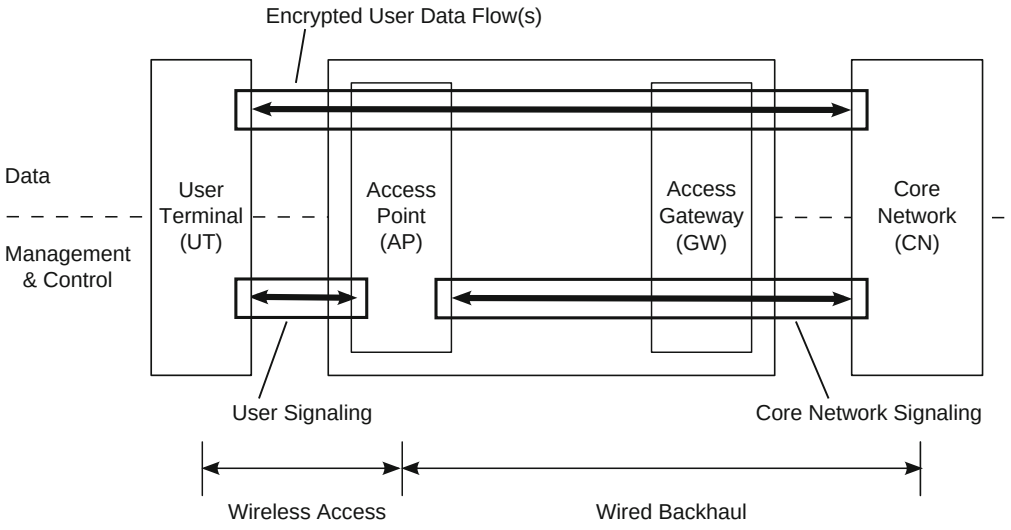

Fig. 1. Security model in traditional wireless access networks.

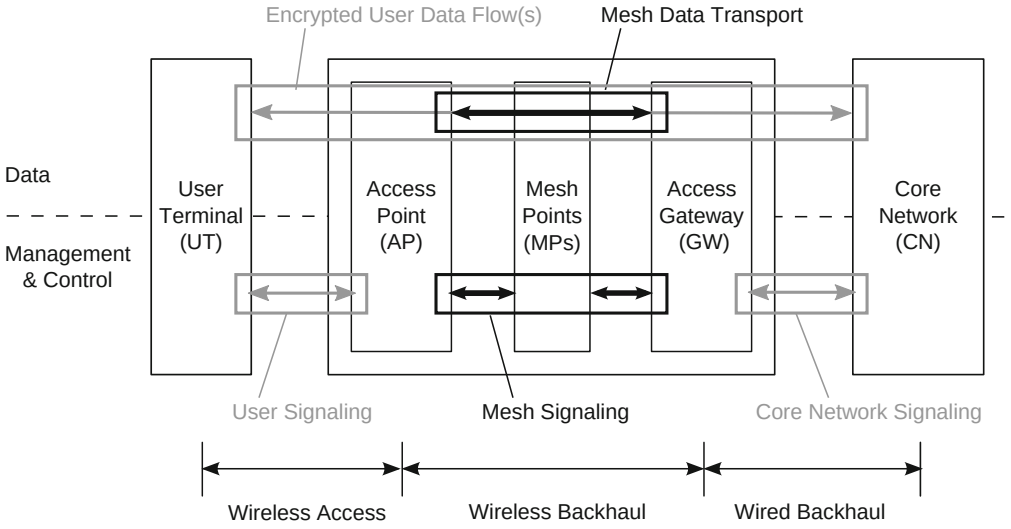

Fig. 2. System security model of a mobile network operator's meshed access network.

in place. Instead, the analysis will focus on these three subsystems:

- the management and control traffic,
- the load-controlled data flows as well as
- the network entities of a WMB architecture.

3.2. Assumptions

To further delimit the scope of this analysis, the following assumptions are made that are in part a consequence of assuming a *carrier-grade* context:

- All network entities of the mesh network are owned and operated by a single administrative entity—the mobile network operator. Mesh nodes (MNs) never deliberately use other MNs under different administration to relay their packets.[3]
- Likewise, UTs are not used for relaying of traffic.
- All network entities are static, so it can be assumed that their neighborhood only changes when a network entity of the WMB is activated or deactivated.
- The physical network entities are tamper-proof, i.e. there are physical countermeasures in place that prevent an attacker with physical access to the device to access information stored in the device. This means, for example, that when a device is opened, it loses all its stored state and cannot be reactivated.
- On the other hand, physical destruction of a network entity or one of its components, e.g. its antennas, is a realistic scenario and has to be taken into account.
- Likewise, it is futile to try to protect wireless links against physical attacks such as jamming, same as against natural impairments like fog and rain. Thus, it is assumed that the considered WMB architecture is able to tolerate the failure of single wireless links and ensure that this only has a transient effect on the service in the remaining part of the network.
- Users have full control of the terminal, which means one cannot expect that the operating system or the firmware of the terminal are a sufficient protection against manipulation of signaling traffic.

[3] For a security architecture that addresses WiFi mesh networks in which nodes belong to different operators see, for example, Toubiana et al. (in press).

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

- The terminal software as well as the software of network entities may be faulty.

3.3. Security objectives

A secure WMB architecture should ensure the following security properties:

Confidentiality: Confidentiality is the absence of disclosure of information to unauthorized individuals or systems. Examples of violations of this property are eavesdropping on confidential communication or inference of confidential information through passive or active traffic analysis.

Integrity: Integrity is the absence of alteration of information by unauthorized individuals or systems. An example of a violation of this property is the manipulation of communication or of data stored inside a network entity.

Authenticity: Authenticity is the establishment that information is genuine and has not been forged or fabricated. An example of a violation of this property is the masquerading of an attacker as a legitimate user of the system to obtain access to confidential information.

Non-repudiation: Non-repudiation means preventing that an individual or system can deny having participated in a transaction with another individual or system. An example of a violation of this property would be that a user denies having established a call to avoid being charged for it. Establishing this property requires, among other things, the existence of charging and accounting mechanisms, which are outside the scope of this work.

Availability: Availability is the delivery of predictable and timely service. The most prominent example of a violation of availability is a DoS attack, typically a resource exhaustion attack.

Privacy: Privacy means the protection of user data from disclosure to unauthorized individuals or systems. This pertains, for example, to information about the user's identity or location. It also pertains to user data traffic, but protection of the latter is typically subsumed under "confidentiality" and this analysis handles it this way, too. An example of a violation of this property is the ability to track a user's location via the network.

3.4. Assets

WMBs store and transport different types of information, such as network state and user data, and require different types of resources for their operation. A security solution therefore needs to protect a wide range of assets:

- User-related assets: user data, (temporary or permanent) user identity, user location.
- Security-related assets: security credentials, session keys.
- Mesh management and control assets: measurement probes for network monitoring, signaling for radio resource management, routing etc.
- Mesh network assets: memory, computing and energy resources of network entities, wireless link bandwidth.

3.5. Actors and threat agents

Trusted *actors* in the sense of this analysis are the users and the operator of the WMB. A user is a person that has an association, for example a pre-paid or post-paid contract with the operator that allows users to use the access services of the mesh. The operator in turn is a person or organization that provides access services to users based on an existing association between them.

There are two kinds of threat agents in the sense of this analysis: The first is faulty software installed on the UTs of a non-malicious user that displays Byzantine faults. This means the UT may, for example, produce invalid protocol messages or not follow the protocol correctly, but does not deliberately try to produce messages that exploit a security vulnerability. The second one is the classical attacker. Attackers may have different levels of sophistication (3GPP, 2005):

- A pass-by cracker would be a single (or a small group of) individuals capable of performing passive or active attacks on radio interfaces using off-the-shelf equipment of limited performance.
- Organized crime or "cyber terrorists" are resourceful organizations, powerful enough to put up false MNs, having a large computing power, etc.
- An agency is an extremely resourceful organization, e.g. a national agency. This type of attacker is not considered further in this analysis, because it is assumed that agencies have more effective means to access or manipulate user-related data, including legal interception.

The two former types of attacker can be further differentiated into whether they are inside attackers, meaning they are authorized to use a service, but abuse it in order to mount an attack, or whether they are outside attackers that do not have or require a minimum level of authorization for their attack. Finally, it is distinguished between a passive attacker, which is an outside attacker that just eavesdrops on communication, and an active attacker that tries to impersonate users or network entities and sends signals or information to mount an attack.

4. Identification of potential security threats

This section analyses the system under test with respect to the potential security threats it may be subject to. As argued in Section 3.1, one can assume that the wireless mesh backbone is embedded into a full mobile network architecture that provides its own security features. The following analysis therefore does not cover security threats targeted at the wireless access link (data and signaling), the core network (data and signaling) or the end-to-end user data protection.[4] Instead it focuses on the wireless mesh-specific part, namely the signaling for management and control as well as the data transport inside the WMB.

4.1. Threats to wireless mesh management and control

Since this work took the common approach to distinguish the WMB architecture between data and management planes, the description of the investigated threats will follow the same structure. Furthermore, the written security objectives in Section 3.3 will be taken as a classification for the treats. All treats will be abbreviated with the capital letter T.

4.1.1. Threats to confidentiality

T1 Eavesdropping mesh management or control frames: An attacker may eavesdrop management or control frames on the wireless links between MNs. The knowledge gained from this could be useful to mount a subsequent active attack on the system, e.g. a deletion attack on a specific protocol message.

[4] For an analysis of these threats, the reader is referred to the 3GPP architecture's security analysis document in 3GPP (2001). The present analysis also follows that document's structure.

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

T2 Masquerading as an MN : An attacker may masquerade as an MN to intercept mesh management and control frames from neighboring MNs. This enables many different forms of active attacks, in particular attacks on routing (e.g. black hole routing attacks).

T3 Passive traffic analysis: An attacker may observe the traffic patterns of mesh management and control frames (e.g. frame lengths, rates, and sequences) sent between MNs to infer information about the employed management and control policies, the system state, etc. This information can be used to discover a suitable attack vector.

T4 Active traffic analysis: An attacker may send signals or protocol frames with valid or invalid protocol fields to an MN and observe the behavior of the MN and the remaining system, e.g. the types and lengths of responses and the latencies after which responses are sent. This can be used to fingerprint the system and its sub-systems, which is useful to discover a suitable attack vector.

4.1.2. Threats to Integrity

T5 Manipulation of mesh management or control frames: An attacker may insert, delete, modify or replay management or control frames on the wireless links between MNs.

4.1.3. Threats to Authenticity

T6 Masquerading as another network entity: An attacker may masquerade as a legitimate MN of the mesh network towards a booting MN that wishes to associate with the network and then hijack his connection after authentication has been performed.

4.1.4. Threats to Availability

T6 Physical intervention: An attacker may use physical means, such as jamming, to prevent management and control frames from being sent between MNs. Also, the attacker could delay transmissions by deleting protocol messages as well as their retransmissions and re-inserting them at any later point in time. Another attack vector could be to create continuous or modulated interference on selected radio links to degrade their link quality and cause network internal management functions to adjust the network topology or traffic flows. This could lead to instability in the mesh network due to topology and route flapping.

T8 Protocol intervention: An attacker may introduce forged protocol messages, e.g. in a routing protocol to announce false or suboptimal routes to cause route flapping or traffic deletion (black hole routing).

T9 Resource exhaustion by outside attacker: An outside attacker may flood Access Points (APs) with authentication/association requests that, while denied, cause authentication and authorization signaling traffic between the AP and its Gateway (GW). This traffic may degrade the system's performance or the service quality of legitimate traffic.

T10 Resource exhaustion by inside attacker: An inside attacker may flood APs or GWs with session requests and release requests that cause admission control and management signaling traffic between the AP and the GW. Likewise, the attacker could provoke high rates of paging messages to be sent by the network. This traffic may degrade the system's performance or the service quality of legitimate traffic.

T11 Resource exhaustion by Byzantine failure: Faulty software on a UT may send invalid or a high rate of valid requests to the system, causing a degradation of the system's performance or the service quality of legitimate traffic.

4.1.5. Threats to user privacy

T12 Traffic analysis: An attacker may perform an active or passive analysis of the management and control messages' time, rate, length, source, and destination to track a user's location.

4.2. Threats on wireless mesh data transport

4.2.1. Threats to confidentiality

T13 Eavesdropping user data frames: An attacker may eavesdrop user data frames on the wireless links between MNs. Even if end-to-end encryption is employed, an eavesdropper may still possibly infer the source, destination and route of user data frames, which could be useful to mount a subsequent active attack on the system, e.g. a deletion attack.

T14 Masquerading as an MN : An attacker may masquerade as an MN to intercept user data frames from neighboring MNs. For instance, this could be used to cause retransmissions and thus higher traffic loads inside the mesh network.

T15 Passive traffic analysis: An attacker may observe the traffic patterns of user data frames (e.g. frame lengths, rates, and sequences) sent between MNs to infer information about the network utilization, load distribution and traffic mix, which could be useful for business intelligence purposes. Furthermore, it could be used to track a user's location.

T16 Active traffic analysis: An attacker may send data frames for authorized or non-authorized users to an MN and observe the behavior of the MN and the remaining system, e.g. the types and lengths of responses and the latencies after which responses are sent. This can be used to fingerprint the system and its sub-systems, which is useful to discover a suitable attack vector.

4.2.2. Threats to integrity

T17 Manipulation of user data frames: An attacker may insert, delete, modify or replay user data frames transported on wireless links between MNs. Even if end-to-end integrity checking is performed by the user or the core network, a manipulation may still cause retransmissions and thus higher traffic loads inside the mesh network.

4.2.3. Threats to authenticity

This threat is equal to threat T6 written in Section 4.1.3.

4.2.4. Threats to availability

T18 Physical intervention: An attacker may use physical means, such as jamming, to prevent user data frames from being sent between MNs. Also, the attacker could delay transmissions by deleting user data frames as well as their retransmissions. Forcing of retransmissions could be used to increase the load and thus decrease the service quality in the mesh network.

T19 Resource exhaustion by inside attacker: An inside attacker may send data traffic such that it maximizes its impact on the service quality of legitimate user data traffic, e.g. using results from adversarial queuing theory, as described by Borodin et al. (1996).

4.2.5. Threats to user privacy

T20 Traffic analysis: An attacker may perform an active or passive analysis of the user data traffic's time, rate, length, source, and destination to track a user's location.

4.3. Threats on wireless mesh network entities

4.3.1. Threats to confidentiality

T21 Unauthorized access to data stored by or forwarded through network entities: An attacker may obtain access to information

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

stored by network entities. Access to network entities may be obtained either locally or remotely, and may involve breaching physical or logical controls.

T22 Fingerprinting: An attacker may perform a passive or active traffic analysis to fingerprint a network entity's protocol stack, operating systems or services. This information can be used to discover a suitable active attack vector.

4.3.2. Threats to integrity

T23 Manipulation of data stored by network entities: An attacker may insert, delete or modify data stored by network entities. Access to network entities may be obtained either locally or remotely, and may involve breaching physical or logical controls.

4.3.3. Threats to authenticity

T24 Masquerading as network entity: An attacker may masquerade as a valid network entity to steal the credentials of a network management entity or to hijack his connection after authentication has been performed.

4.3.4. Threats to availability

T25 Physical intervention: An attacker may physically destroy or manipulate a network entity or one of its parts (e.g. a single antenna). Furthermore, he could deliberately interrupt the network entities power supply to deactivate it or to force it to restart.

T26 Resource exhaustion by an outside attacker: An outside attacker may abuse faults in the protocol stack to reduce or even exhaust a network entity's memory, processing or energy (if battery-powered) resources. This could degrade the system's availability to legitimate users.

T27 Resource exhaustion by an inside attacker: An inside attacker may abuse faults in the protocol stack or send a flood of service requests to reduce or even exhaust a network entity's memory, processing or energy (if battery-powered) resources. This could degrade the system's availability to legitimate users.

T28 Resource exhaustion by Byzantine failure: Faulty software on a UT may send invalid or a high rate of valid requests to a network entity that reduce or even exhaust its memory, processing or energy (if battery-powered) resources. This could degrade the system's availability to legitimate users.

4.3.5. Threats to user privacy

T29 Browsing of user-related data stored by network entities: An attacker may obtain access to information stored or cached in network entities that allows him to infer private information about a user, e.g., to connect the user's identity with a temporary terminal identifier to track user movement or service usage profiles.

5. Risk assessment of security threats

After defining all investigated security threats in the previous section all threats will be assessed regarding their risks to the security of the WMB. The main goal of the risk assessment activity is to evaluate the identified potential threats and assign risks to them. They thus become comparable with each other. Furthermore, this allows major risks to be identified.

For the risk assessment, we adopt the methodology defined by European Telecommunications Standards Institute (ETSI)'s Security Techniques Advisory Group (STAG), as described in ETSI TC-STAG (1996):

- Following this methodology, each threat is first evaluated with respect to the impact I it would have on each threatened subject if it occurred. The impact is appraised on a scale from one to five, with one being the lowest impact.
- Next, the likelihood of occurrence O is evaluated, again on a scale from one to five with one being the lowest likelihood.
- Multiplying the level of impact with the level of likelihood yields the so-called exposure factor, i.e. the product of I and O.
- Finally, threats are ranked by their exposure factor and major risks—those having an exposure factor above a certain threshold (here: 10)—are identified. The result is summarized in Table 3.

The five levels of impact and likelihood need to be made operational by defining them within the context of a specific application domain. Here, we adopt the levels for a 3GPP environment, as described in 3GPP (2005). The employed levels for threat impact and threat likelihood are listed in Tables 1 and 2, respectively.

The following list presents the risk assessment for each identified potential threat. Where applicable, it also contains forward references (→Rx) to the list of security requirements in Section 5.5. Note that in particular the appraisal of the likelihood of occurrence is time-variant and depends on border conditions like the computational power available to a "resourceful organisation" or the skills and automated tools available to a

Table 1
Threat impact levels used for risk assessment.

Level	Impact	Example
1	Minimal	Threats that would not imply anything for user privacy, Quality of Service (QoS) or charging, e.g. being able to occasionally increase a phone's transmit power.
2	Small	Threats that, if realized, only cause very small annoyance for a single user during a short period of time.
3	Medium	Local threats, e.g., DoS attack targeted at a small set of nearby MNs. Could occasionally lead to single instances of incorrect charging data.
4	High	Something that, if realized, would be mentioned in IT/telecom media.
5	Very high	Something that would make front-page news, seriously damaging the trust in mobile networks, either from users' or operators' point of view, e.g. complete loss of privacy and/or robust charging.

Table 2
Threat likelihood levels used for risk assessment.

Level	Likelihood	Example
1	Negligible	Attack successful with a probability comparable to guessing/breaking an (at least) 80-bit key, or requiring resources equivalent to breaking such a key. Alternatively, requiring full control of some critical function, e.g. the Authentication, Authorisation and Accounting (AAA) infrastructure, from the "outside".
2	Unlikely	Organized crime with considerable resources would only occasionally be able to mount a successful attack.
3	Medium	Organizations capable of erecting rogue WMB equipment, e.g. MNs, are likely to be able to succeed.
4	High	Qualified/resourceful individuals or small groups, e.g. capable of manipulating consumer products on a limited scale, could succeed.
5	Almost certain	The attack is performed realized by single, averagely skilled "hackers" with standard PC/phone resources, possibly using "attacking tools" developed by someone else, found on the Internet.

Adapted from 3GPP (2005).

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

"pass-by" cracker. This risk assessment therefore requires re-evaluation if border conditions change in the future.

5.1. Threats to wireless mesh management and control

5.1.1. Threats to confidentiality

T1 *Eavesdropping mesh management or control frames*: Assuming a proper and robust encryption of management and control frames (→R1), the likelihood of occurrence is negligible, but a successful attack would make headlines in IT/telecom media if realized.

Likelihood: 1 (negligible), Impact: 4 (high)

T2 *Masquerading as a MN* : Assuming proper mutual authentication of MNs (→R2), the likelihood of successfully masquerading as a MN, e.g. to intercept management and control frames, is negligible. However, a successful attack would make headlines in IT/telecom media if realized.

Likelihood: 1 (negligible), Impact: 4 (high)

T3 *Passive traffic analysis*: A passive traffic analysis to find vulnerabilities of the WMB requires individuals or groups with the resources and the skills to sniff and analyze mesh traffic. The impact of this analysis is minimal, as long as this attack is not used to prepare an active attack.

Likelihood: 4 (high), Impact: 1 (minimal)

T4 *Active traffic analysis*: An active traffic analysis to find vulnerabilities of the WMB requires individuals or groups with the resources and the skills to sniff and analyze mesh traffic. The impact of this analysis is small due to occasional impairment of network service, as long as this attack is not used to prepare an active attack.

Likelihood: 4 (high), Impact: 2 (small)

5.1.2. Threats to integrity

T5 *Manipulation of mesh management or control frames*: Assuming a proper and robust mutual authentication of MNs →R1) and checking for integrity and validity of mesh management and control frames (→R3), the likelihood of occurrence is negligible, but a successful attack could affect the service availability of the whole network and make front-page headlines if realized.

Likelihood: 1 (negligible), Impact: 5 (very high)

5.1.3. Threats to authenticity

T6 *Masquerading as another network entity*: Assuming a proper and robust encryption of management and control frames (→R1), the likelihood of occurrence is negligible, but a successful attack could affect the service availability of the whole network and would make front-page headlines if realized.

Likelihood: 1 (negligible), Impact: 5 (very high)

5.1.4. Threats to availability

T7 *Physical intervention*: An intelligent jamming that can cause network-wide instabilities requires a higher level of sophistication than merely taking down a single mesh link through jamming, because the characteristics and behavior of the targeted mechanism have to be taken into account. Resource requirements are moderate, though, and a successful attack could affect the service availability of the whole network and is very likely to receive coverage in at least in the IT/telecoms media.

Likelihood: 4 (high), Impact: 4 (high)

T8 *Protocol intervention*: Assuming a proper and robust authentication (→R1) and checking for integrity and validity (→R3), the likelihood that an attacker manages to inject malicious protocol messages is negligible, but a successful attack could affect the service availability of the whole network and would make front-page headlines if realized.

Likelihood: 1 (negligible), Impact: 5 (very high)

T9 *Resource exhaustion by outside attacker*: An authentication/association flooding attack is relatively easy to perform as the necessary tools are simple to create or obtain. Also the risk of exposure of the attacker is comparatively low. Assuming measures to rate control the acceptance of user signaling as well as proper performance dimensioning and implementation of the AP (→R6), the impact of this attack should be small.

Likelihood: 5 (almost certain), Impact: 2 (small)

T10 *Resource exhaustion by inside attacker*: While, for example, the tools for an attack by flooding of call setup/release requests are simple to create or obtain, the necessity for authorized network access by multiple attackers requires quite some resources and has a high risk of exposure. Assuming measures to rate control the acceptance of user signaling as well as proper performance dimensioning and implementation of the AP (→R6), the impact of this attack should be small, though.

Likelihood: 3 (medium), Impact: 2 (small)

T11 *Resource exhaustion by Byzantine failure*: While software faults causing byzantine behavior are likely to exist in user terminals, it is unlikely that these cause floods of valid or invalid requests. Assuming measures to rate control the acceptance of user signaling as well as proper performance dimensioning and implementation of the AP (→R6), the impact of this attack should be small, though.

Likelihood: 2 (unlikely), Impact: 2 (small)

5.1.5. Threats to user privacy

T12 *Traffic analysis*: A traffic analysis of management and control traffic, for example to track user locations, requires individuals or groups with significant resources and the skills to sniff and analyze mesh traffic on a relatively large number of wireless mesh links. The effort for this attack also seems hardly worth the effort, as simpler methods exist to track user locations. Also, the impact of this attack would be relatively small, as users are typically little concerned with location privacy and expect public authorities to be able to obtain this information from the operators anyway.

Likelihood: 2 (unlikely), Impact: 2 (small)

5.2. Threats on wireless mesh data transport

5.2.1. Threats to confidentiality

T13 *Eavesdropping user data frames*: Assuming proper and robust encryption of user data (→R4), the likelihood of occurrence is negligible, but a successful attack would make front-page headlines.

Likelihood: 1 (negligible), Impact: 5 (very high)

T14 *Masquerading as a MN* : Assuming proper mutual authentication of MNs (→R2) the likelihood of successfully masquerading as a MN to intercept user data frames is negligible. However, a successful attack would make front-page headlines if realized.

Likelihood: 1 (negligible), Impact: 5 (very high)

T15 *Passive traffic analysis*: A passive traffic analysis, for example to track user locations or obtain business intelligence, requires individuals or groups with significant resources and the skills to sniff and analyze mesh traffic on a relatively large number of wireless mesh links. The effort for this attack also seems hardly worth the effort, as simpler methods exist to obtain this information. Still, this knowledge might be somewhat interesting to an operator's competitor.

Likelihood: 2 (unlikely), Impact: 3 (medium)

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

T16 *Active traffic analysis*: An active traffic analysis to find vulnerabilities of the WMB requires individuals or groups with the resources and the skills to sniff and analyses mesh traffic. This impact of the analysis is small due to occasional local impairment of network service, as long as this attack is not used to prepare an active attack.

Likelihood: 4 (high), Impact: 2 (small)

5.2.2. Threats to integrity

T17 *Manipulation of user data frames*: Assuming a proper and robust mutual authentication of MNs (→R1) and checking for integrity of transported user data frames (→R5), the likelihood of occurrence is negligible, but a successful attack would make front-page headlines if realized.

Likelihood: 1 (negligible), Impact: 5 (very high)

5.2.3. Threats to availability

T18 *Physical intervention*: A selective jamming to degrade user service requires a higher level of sophistication than merely taking down a single mesh link through jamming, but is feasible by a resourceful, qualified attacker. The attack would be of small impact, though, as it would merely lead to a local degradation of user service.

Likelihood: 4 (high), Impact: 2 (small)

T19 *Resource exhaustion by inside attacker*: Assuming a proper policing of user data at the ingress point (→R7), an attack in which an insider causes a resource exhaustion by flooding with user data requires considerably high amounts of expertise and resources. It might then potentially have an impact on the user service in the whole network.

Likelihood: 2 (unlikely), Impact: 3 (medium)

5.2.4. Threats to use privacy

T20 *Traffic analysis*: A traffic analysis of user data traffic to track user locations requires individuals or groups with significant resources and the skills to sniff and analyze mesh traffic on a relatively large number of wireless mesh links. The effort for this attack also seems hardly worth the effort, as simpler methods exist to track user locations. Also, the impact of this attack would be relatively small, as users are typically little concerned with location privacy and expect public authorities to be able to obtain this information from the operators anyway.

Likelihood: 2 (unlikely), Impact: 2 (small)

5.3. Threats on wireless mesh network entities

5.3.1. Threats to confidentiality

T21 *Unauthorized access to data stored by or forwarded through network entities*: Assuming proper mutual authentication of MNs (→R2) the attacker would have to find a vulnerability in the implementation of the network stack or the limited services running on the network entities, which requires a relatively high level of expertise. A successful attack with read access to the very limited information on network entities is likely to receive coverage in IT/telecoms media if realized.

Likelihood: 3 (medium), Impact: 4 (high)

T22 *Fingerprinting*: Fingerprinting a network element's protocol stack requires qualified individuals with a decent amount of resources. The effect of a successful attack is knowledge about potential vulnerabilities of the system, but the impact of this is minimal, as long as this knowledge is not used to prepare an active attack.

Likelihood: 4 (high), Impact: 1 (minimal)

5.3.2. Threats to integrity

T23 *Manipulation of data stored by network entities*: Assuming proper mutual authentication of MNs (→R2) the attacker would have to find a vulnerability in the implementation of the network stack or the limited services running on the network entities, which requires a relatively high level of expertise. A successful attack that allows manipulating the charging and accounting records is likely to receive good coverage in the general media if realized.

Likelihood: 3 (medium), Impact: 5 (very high)

5.3.3. Threats to authenticity

T24 *Masquerading as network entity*: Assuming proper mutual authentication of MNs (→R2) the likelihood of successfully masquerading as network entity, for example to hijack network management connections, is negligible. However, a successful attack would give the attacker control of the network and would likely result in negative press coverage in IT/telecom media if realized.

Likelihood: 1 (negligible), Impact: 4 (high)

5.3.4. Threats to availability

T25 *Physical intervention*: A physical destruction of (parts of) network entities requires very little sophistication and is therefore almost certain to occur deliberately or accidentally. The impact of this attack is moderate, potentially affecting those neighbors that forward traffic via this AP. This assumes the network entity is not a single point of failure affecting the availability of the whole network (→R8).

Likelihood: 5 (almost certain), Impact: 3 (medium)

T26 *Resource exhaustion by an outside attacker*: Exhausting the resources of an AP from the outside requires a very skilled and resourceful individual or group. If the attack succeeds, the impact is moderate, affecting the availability of the attacked AP and potentially of those neighbors that forward traffic via this AP. This assumes the network entity is not a single point of failure affecting the availability of the whole network (→R8).

Likelihood: 4 (high), Impact: 3 (medium)

T27 *Resource exhaustion by an inside attacker*: Exhausting the resources of an AP from the inside requires a very skilled and resourceful individual or group with the capability of obtaining authorized network access by multiple attackers and has a high risk of exposure. If the attack succeeds, the impact is moderate, affecting the availability of the attacked AP and potentially of those neighbors that forward traffic via this AP. This assumes the network entity is not a single point of failure affecting the availability of the whole network (→R8).

Likelihood: 3 (medium), Impact: 3 (medium)

T28 *Resource exhaustion by Byzantine failure*: While faults are likely to exist in user terminals, it is unlikely that they cause resource exhaustion in a properly implemented network entity. If the attack succeeds, the impact is moderate, affecting the availability of the attacked AP and potentially of those neighbors that forward traffic via this AP. This assumes the network entity is not a single point of failure affecting the availability of the whole network (→R8).

Likelihood: 2 (unlikely), Impact: 3 (medium)

5.3.5. Threats to user privacy

T29 *Browsing of user-related data stored by network entities*: Assuming proper mutual authentication of MNs (→R2) the attacker would have to find a vulnerability in the implementation of the network stack or the limited services running on the network entities to gain access, which requires a relatively high level of expertise. The impact of this attack would be relatively

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

small as users are typically little concerned with location privacy and expect public authorities to be able to obtain this information from the operators anyway.

Likelihood: 3 (medium), Impact: 2 (small)

5.4. Summary

The results of the risk assessment are summarized and ranked in Table 3. The first five entries are major risks to a WMB architecture. Interestingly, only one (the highest ranking) of the major risks involves an attack on wireless mesh links or the information they transport: causing network instabilities through intelligent jamming of multiple wireless links. Another major risk is a physical attack on network entities which requires physical countermeasures. The last group of attacks involves exploiting faults in the implementation of network entities (T12 and T23) or design flaws that make network entities open to denial of service attacks (T26).

5.5. Derived requirements

From the previous analysis, we shortly summarize the following derived minimum security requirements:

R1 All management and control traffic MUST be robustly encrypted when sent over a wireless link. This also applies to all data sent to merely 'probe' the existence or quality of a wireless link.

R2 All MNs MUST be mutually authenticated before exchanging any other management or control data.

R3 All received management and control messages MUST be checked for authenticity, integrity and validity before any further processing takes place.

R4 All user traffic transported in internal mesh flows MUST be robustly encrypted when sent over a wireless link.

R5 All user traffic frames forwarded between two MNs MUST be checked for authenticity (of the previous hop) and integrity.

R6 The acceptance and processing of user requests, such as authentication and association or call set up requests, MUST be rate controlled and the network entities MUST be properly dimensioned with respect to their memory, CPU and energy resources.

R7 All user traffic MUST be policed at the ingress point.

R8 Single points of failure MUST be avoided. All functions MUST be able to tolerate failures of single MNs or links.

R9 All mechanisms and protocols MUST be robust to losses and late delivery of protocol messages.

R10 The system MUST NOT keep state for unauthenticated individuals or systems and it MUST NOT keep state for any request that failed in order to reduce the chance of a resource exhaustion attack.

Table 3
Exposure factors and rankings of identified potential security risks.

Threat	Description	I	O	$I * O$	Rank
T7	Intelligent jamming to cause instabilities	4	4	16	1
T23	Manipulation of data on network entities	5	3	15	2
T25	Physical destruction of network entities	3	5	15	
T21	Unauthorized data access in network entities	4	3	12	4
T26	AP resource exhaustion by outside attacker	3	4	12	
T9	Authentication/association flooding	2	5	10	6
T27	AP resource exhaustion by inside attacker	3	3	9	7
T4	Active management traffic analysis	2	4	8	8
T16	Active user traffic analysis	2	4	8	
T18	Selective jamming to degrade user service	2	4	8	
T10	Flooding of call setup/release requests	2	3	6	11
T15	Passive traffic analysis for BI	3	2	6	
T19	Resource exhaustion by user data flooding	3	2	6	
T28	Resource exhaustion by Byzantine failure	3	2	6	
T29	Browsing of user-related data	2	3	6	
T5	Manipulation of mesh management frames	5	1	5	16
T6	Masquerading as another network entity	5	1	5	
T8	Injecting malicious protocol messages	5	1	5	
T13	Eavesdropping user data frames	5	1	5	
T14	Masquerading as a MN to intercept data	5	1	5	
T17	Manipulation of user data frames	5	1	5	
T1	Eavesdropping management frames	4	1	4	22
T2	Masquerading to intercept mgmt. frames	4	1	4	
T3	Passive traffic analysis to find vulnerabilities	1	4	4	
T11	Byzantine failures causing signaling flood	2	2	4	
T12	Traffic analysis of signaling for user tracking	2	2	4	
T20	Traffic analysis of data for user tracking	2	2	4	
T22	Fingerprinting of network entities	1	4	4	
T24	Masquerading to hijack management connections	4	1	4	

I = Impact, O = Likelihood.

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

6. Recommendations for the architectural design

For some of the security requirements identified in Section 5.5, namely R1–R5, standard security solutions exist that can be employed to fulfill these requirements. For requirements R6–R10, in contrast, no standard security solutions exist. These need to be dealt with by "security by design", which means to design both architecture and implementation in a way that precludes the respective threats from the beginning. This section provides some general recommendations on how to achieve these goals.

6.1. Avoid state without authorization

One type of DoS attacks is based on resource exhaustion. The most important resources of a network entity are its memory space, its processing power and its energy supply (if battery-powered). For the communication between nodes, bandwidth is an important resource as well. To mount a resource exhaustion attack, an attacker tries to identify a system's bottleneck resource and then attempts to occupy all of this resource, so that none or only an insufficient share of this resource remains for legitimate users.

A typical example is storing per-user information upon a request by an unauthenticated user. An attacker will then try to flood the system with this type of request, changing its identity for each request, until the buffer space for this type of request is depleted. The same issue can also occur for authenticated users, though, if, for example, the vulnerable system stores state for each call set-up request and the number of requests per user is not limited.

6.2. Control signaling rates

Memory is just one of the resources to be protected from exhaustion. Attacks on CPU and communication bandwidth try to submit requests to the system at a higher rate than the system can process them. Merely increasing the power of the system so that it can process requests more quickly is both costly and typically futile, resulting in an arms race with the attacker.

The solution is to control the rate of requests at the ingress into the system. This can be a natural rate control, e.g. when the bandwidth of the access link limits the number of messages that can be sent on it per second. Otherwise the rate of requests needs to be artificially throttled below the rate at which the system can service requests. This also limits the amount of bandwidth consumed for signaling, as many requests will involve sending signaling traffic across the mesh between the access points and the gateways.

6.3. React moderately to link degradation

In another one of the studied attack scenarios, an attacker attempts to leverage resilience features of a WMB architecture to make a DoS attack based on physically jamming radio links more efficient. Assume the attacker just jams a wireless mesh link long enough to cause the internal mesh functions to detect a link QoS degradation and perform a link adaptation, a re-routing of user flows or even a change in the logical topology of the network. Afterwards, the attacker does the same at a second location in the network to which most of the traffic was shifted. The attacker may then succeed to keep the network in an unstable state while investing very little resources compared to jamming a large number of links concurrently.

Although this type of attack is not possible to completely avoid, it can be made more difficult. This requires that the functions dealing with adaptation to interference make the minimum necessary adaptations that interfere with traffic and network topology as little as possible. Furthermore, it is useful to employ a hysteresis to reduce the susceptibility to a "ping-pong effect".

6.4. Avoid single points of failure

If the goal of an attack is to violate the availability of the mesh network, an attack vector with high likelihood of success is a physical attack on mesh network entities. This requires overcoming the physical countermeasures and then either destroying the network entity or its communication interfaces or simply interrupting its power supply.

The effectiveness of such an attack depends on whether the targeted network entity is a single point of failure or not. In the worst case, the attacked network entity is crucial for the operation of a large part or even the whole mesh network. As an example, consider the case of a mesh network design with a single gateway and the call setup function in the core network or a network design with multiple gateways, but only one of them hosting a centralized routing function.

Note that to solve the vulnerability described in the last example it is not sufficient to introduce multiple gateways, each one having its own centralized routing function and each one being responsible for a given part of the mesh network, as this would limit the problem to a smaller area, but not solve the problem. Instead, the function has to be designed for real redundancy, i.e. any GW has to be able to take over the role of at least its neighboring GWs, should that become necessary.

6.5. Expect failures

Even in a design that avoids single points of failure it is good to "design for failures". Failures are not only a result of a deliberate attack, but also happen due to faulty software, overheating, etc. A robust design therefore treats failures of mesh points, antennas, wireless links, etc. as something that cannot be avoided, but which on the contrary is expected to occur. Thus, the design should be such that mesh points can be rebooted quickly and reinserted into the mesh topology by recovering the necessary state from neighboring mesh points or from a central repository.

7. Conclusions

The objective of this security analysis has been to identify potential security threats to a WMB architecture and to provide recommendations on how to resolve the underlying security issues for the cases that standard security solutions do not exist. The analysis started with delimiting the scope of the system under study. The context of carrier-grade WMBs helped to focus the scope, because it makes it reasonable to assume that several security features are already in place and that furthermore MNs are controlled by the operator. The following systematic analysis then identified 29 potential security threats, out of which five were classified as major risks following a risk assessment. These major risks are:

- Intelligent jamming to cause routing and self-configuration functions to make frequent changes to the routing of traffic pipes and to the mesh topology, respectively, leading to an unstable network.
- Physical destruction of network entities or interruption of the power supply.

Please cite this article as: Zdarsky FA, et al. Security analysis of wireless mesh backhauls for mobile networks. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.03.029

- Manipulation of data on network entities.
- Unauthorized access to data on network entities.
- Exhaustion of a network entity's resources by an outside attacker.

An interesting observation of the risk assessment is that only one (the highest ranking) of the major risks involves an attack on wireless mesh links or the information they transport. The remaining ones target potential vulnerabilities of the network entities and require physical countermeasures as well as good architecture and implementation design practices (security by design). The identification of potential security threats further led to the definition of several security requirements. A part of these security requirements can be met by employing standard security solutions like Internet Protocol Security (IPSec) for end-to-end message authentication, integrity and encryption. The other part has to be met by "security by design" and several recommendations have been given to reduce the risk of vulnerabilities in the architecture design.

Acknowledgements

This work was partially funded by the European Commission within the 7th Framework Program in the context of the ICT project CARMEN (2008) under Grant Agreement no. 214994. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Carrier Grade Mesh Networks (CARMEN) project or the European Commission.

References

3GPP. Security threats and requirements. 3GPP TS 21.133 (V4.1.0); 2001.
3GPP. Access security review. 3GPP TR 33.801 (V1.0.0); 2005.
Adoba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H. Extensible authentication protocol (EAP). IETF RFC 3748; 2004.
Adoba B, Simon D, Eronen P. Certificate management messages over CMS (CMC): Compliance requirements. IETF RFC 5247; 2008.
Borodin A, Kleinberg J, Raghavan P, Sudan M, Williamson DP. Adversarial queuing theory. In: 28th ACM Symposium on Theory of Computing (STOC); 1996. p. 376–85.
CARMEN. CARrier grade MEsh Networks. In: ICT Project of the EC's 7th Framework Programme; 2008.
iGillott Research. 3G mobile network security. White Paper; 2007.
ETSI TC-STAG. Security requirements capture. ETSI ETR 332; 1996.
Hu YC, Perrig A. A survey of secure wireless ad hoc routing. IEEE Security and Privacy 2004;2(3):28–39.
Naveed A, Kanhere S. Security vulnerabilities in channel assignment of multi-radio multi-channel wireless mesh networks. In: IEEE Global Telecommunications Conference (GLOBECOM'06); 2006. p. 1–5.
Ren K, Yu S, Lou W, Zhang Y. PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks. IEEE Transactions on Parallel and Distributed Systems 2010;21(2):203–15.
Toubiana V, Labiod H, Reynaud L, Gourhant Y. A global security architecture for operated hybrid WLAN mesh networks. Computer Networks 2010; 54(2):218–30.
Yan Y, Cao J, Li Z. Stochastic security performance of active cache based defense against dos attacks in wireless mesh network. In: Second International Conference on Advances in Mesh Networks (MESH 2009); 2009. p. 30–6.
Zhang Y, Fang Y. ARSA: an attack-resilient security architecture for multihop wireless mesh networks. IEEE Journal on Selected Areas in Communications 2006;24(10):1916–28.