Time behaviour and network encumbrance due to authentication in wireless mesh access networks

Andreas Roos, Sabine Wieland
University of Applied Sciences Leipzig
04277 Leipzig, Germany
{Roos, Wieland}@fh-telekom-leipzig.de

Andreas Th. Schwarzbacher
Dublin Institute of Technology
Dublin 8, Ireland
Andreas.Schwarzbacher@dit.ie

Bangnan Xu
T-Systems Enterprise Services GmbH
64295 Darmstadt, Germany
Bangnan.Xu@t-systems.com

Abstract—In this paper we investigate the authentication behaviour of mobile nodes within wireless mesh access networks. This work evaluates the authentication time and the requirements to achieve carrier grade mesh networks, considering mobility of mobile nodes. Three authentication architectures, such as centralised, hierarchical and distributed, are presented. This paper work proposes a fundamental architecture for mesh networks that provides mobility support. Furthermore, general aspects and requirements to achieve carrier grade mesh networks are discussed.

I. INTRODUCTION

Wireless mesh networks (WMNs) are able to realise flexible and extendable broadband wireless Internet access in a cost efficient manner. The ability to forward data over multiple hops at a high data rate eliminates the requirements to connect each access point to a wired infrastructure.

But wireless mesh networks are still in their infancy. Further aspects, e.g. authentication, authorisation and accounting (AAA), security support and quality of service (QoS), are key factors to fulfil carrier grade requirements, beside broadband access and cost efficiency. The capability of WMNs is measurable by means of “Triple Play” (voice, video and data) service provisioning compared to existing network infrastructures. Security support, to ensure customers privacy, integrity, authenticity, non-repudiation as well as confidentiality of customer data, is an additional aspect towards carrier grade mesh networks. Customers will only trust new services if their privacy is guaranteed. However, many issues are still unsolved and need further investigations [1], e.g. suitable concepts and mechanisms for mesh network access control and secure internal mesh network communication. Additionally, multi-hop routing mechanisms of WMNs can be influenced by manipulated routing messages. Moreover, approaches to achieve secure communication within WMNs, e.g. mutual authentication between each mesh node or trust based authentication [2], [3] need further investigations regarding scalability, efficiency and usability.

Broadband wireless Internet access and service provisioning in moving vehicles becomes more and more important [4] and [5]. But broadband wireless access in high speed transportation is challenging [6]. It is essential for wireless networks to provide services of the same quality as wired access networks. As a result, mobility support of wireless mesh networks is necessary to connect fast moving trains to the Internet. For example, WMNs are able to provide broadband coverage alongside a railway or a highway to establish Internet connectivity. But the capability of mobility support needs further investigations regarding AAA functionalities. At this stage the focus is on three authentication architectures for WMNs, such as centralised, hierarchical and distributed authentication approach. The appointment of suitable locations of access decision mechanisms and AAA information is challenging and has to be investigated regarding different access scenarios, such as fixed, nomadic or mobile access of users.

This paper describes fundamental requirements of AAA for railway mesh networks. In this context three different authentication architectures are presented and the benefits and drawbacks of each architecture are discussed. The access scenarios, such as mobile, fixed and nomadic access, and their requirements on the authentication architectures are considered as well. Investigation of initial static simulation results, e.g. authentication data and time behaviour, aims to propose fundamental statements for locating AAA mechanisms within wireless mesh network infrastructures. The rest of this paper is organised as follows: Section II presents a general overview of a WMN infrastructure. Three authentication architectures for WMNs are discussed in section III. Section IV evaluates initial authentication data and time behaviour results within WMNs. Results of Section IV are discussed in the context of the authentication architectures in Section V.

II. AAA IN WIRELESS MESH NETWORKS

The mesh components, such as mesh base station (M-BS) and mesh subscriber station (M-SS), build the WMN backbone. In the event that no access control mechanisms are implemented within the WMN, a mobile node (MN) or another M-SS is able to get network access without authentication. Regarding the requirements of carrier grade mesh networks this behaviour does not fulfill the conditions even not in a fundamentally manner. Due to this, it is essential to integrate network access control mechanisms within WMN infrastructures. Basically, there are two possible major types of authentication in WMNs. The first type of authentication is

11This work is partly supported by the German Ministry of Education and Research (BMBF)
responsible for customer/MN authentication and authorisation to provide mesh network access control and the second type of authentication provides inter mesh point authentication and authorisation to establish a secure mesh network backbone. Goal of both authentication types is the avoidance of mesh network access by malicious MNs or M-SSs and thus, the protection of the mesh backbone. The focus of this paper is on the first authentication type, the MN authentication.

There are different authentication techniques, such as the IEEE Standard 802.1X, which defines a port based network access control mechanism on layer 2, as well as the protocol for carrying authentication for network access (PANA), that provides network access control of clients and routers in general. However, it is challenging to provide multi-hop authentication, like discussed in [7] and [8]. Figure 1 shows a mesh access network infrastructure. The M-SSs of the wireless mesh access network are connected to the Internet via the M-BS. A mobile node connects to a M-SS and thus, to the mesh access network. The coverage of a single M-SS depends on the radius, \( r \), of the radio cell. In this infrastructure a MN moves with the speed, \( v \), through the radio cell towards the moving direction. Access to the Internet will be provided after successful authentication of the MN. Each change of the attachment point within the mesh network needs a new authentication of the MN.

III. AUTHENTICATION SCENARIOS IN WIRELESS MESH NETWORKS

With regard to carrier grade and railway mesh networks it is important to provide only authorised customers access to the network. The efficiency of access decision mechanisms interrelates with its location within the network architecture. Thus, the location of access decision mechanisms is of importance for WMNs. There are several approaches to distribute access decision mechanisms within a WMN architecture, three possible approaches are:

- Central approaches - access decision mechanism is located in the M-BS between mesh access network and existing infrastructure network.
- Hierarchical approaches - access decision mechanisms are hierarchical distributed between M-BS and M-SS within the mesh network additionally to the M-BS.
- Distributed approaches - access decision mechanisms are located in each M-SS within the mesh network.

Authentication and access control decisions belong together with exchange of authentication messages. This exchange leads to data increasing within the network. Based on this, the QoS management might be influenced due to a changing resource behaviour. Network authentication is also important for mobility support of mobile clients. Mobility demands for short authentication times to provide seamless handover between different points of attachments or different access networks respectively. The location of the access decision function seems to be able to impact the resource behaviour of routes in a network and to impact the authentication time behaviour of each mobile client as well [9]. As a result, the evaluation of suitable access decision locations for WMNs is essential to achieve efficient access control to support QoS and mobility in mesh networks. Besides the location of access decision mechanisms, it is mandatory to improve the authentication mechanisms itself to reduce the authentication time and consequently to enhance the handover behaviour.

The following subsections describe the characteristics of the three different mesh AAA architectures in general. Figure 2 presents an overview of the authentication architectures of mobile nodes. An assumption for the further consideration and investigations is, the M-BS acts a temporal AAA server and contains all relevant AAA information, such as user data and user profiles, needed for carrying out a user authentication and authorisation. This means, the mesh base station AAA (M-AAA) server needs not to request the central AAA server within the Internet for further AAA information to provide network access decisions. The mesh network access control is provided by each attachment point and is located within each M-SS. The access decision of the M-AAA server manages the access control function within the M-SS. Finally, the M-SS controls the mesh network access of a MN. The collected accounting information during a online session is send from the M-AAA server to the central AAA server, after the session is finished by the MN. However, information needed for MN network access decision still remains within the M-AAA server until the MN leaves the range of the wireless mesh network.
A. Centralised authentication architecture for WMNs

The central authentication architecture consists of multiple M-SSs and a M-AAA server within a M-BS, that provides access decisions for the whole WMN. AAA information are temporally stored within the M-AAA server. In the case of MN connecting to a mesh network attachment point, the M-SS receives an access request from the MN and forwards the request to the M-AAA server. The M-AAA performs the MN authentication and authorisation and sends the result of access decision back to the M-SS. Based on this decision the M-SS allows or denies network access of MN.

B. Hierarchical authentication architecture for WMNs

The hierarchical authentication architecture is based on the same architecture, like the central architecture and consists of multiple M-SSs and a M-AAA server within a M-BS, that provides network access decisions. The difference between both architectures is the hierarchical access decision function (HAD). The HAD is located within a M-SS and grades the M-SS up to a further temporal AAA server (H-AAA) of the mesh network. Several HADs can be located within a mesh network and is at least one hop away from the MNs point of attachment. In the case of a MN connecting to a mesh network attachment point, the M-SS receives an access request from the MN and forwards the request to the next surrounded H-AAA server. The H-AAA server provides the network access decision of the MN if the AAA information of the MN is temporal stored within the H-AAA server. This means, in the case of the first access request of a mesh node the H-AAA has no MN AAA information to carry out the network access decision. Based on this, the H-AAA server requests the M-AAA server for the relevant AAA information of the MN and stores these information. Finally, the HAD performs the MN authentication then authorisation and sends the access decision back to the M-SS. Based on this decision the M-SS allows or denies network access of MN.

C. Distributed authentication architecture for WMNs

The distributed authentication architecture is based on the same architecture, as the central architecture and consists of multiple M-SSs and a M-AAA server within a M-BS. The difference between both architectures is the distributed access decision function (DAD). The DAD is located within each M-SS and grades the M-SS up to a further temporal AAA server (D-AAA) of the mesh network. Many DADs would be located within a mesh network. In the case of a MN connecting to a mesh network attachment point, the D-AAA server of the M-SS carries out the network access decision. The D-AAA server provides network access decision if the AAA information of the MN is temporal stored within the D-AAA server. In the event of the first access request of a MN the D-AAA server has no MN AAA information to carry out a network access decision. In this case the D-AAA server requests from the M-AAA server the relevant AAA information of the MN and stores these then. Finally, the DAD within the M-SS performs the MN authentication, authorisation and delivers the access decision to the network access control mechanism of the M-SS. Based on this decision the network access is allowed or denied.

IV. AUTHENTICATION DATA AND TIME BEHAVIOUR FOCUSING WMNs

The location of the network access decision function seems to be able to influence the authentication time behaviour of MN and data behaviour within a network [9]. However, a suitable location depends on the access scenario of MNs, such as fixed, nomadic or mobile access, as well. Fast authentication times are good in general, but not really necessary for fixed and nomadic access. However, with focus on mobility fast authentication times are certainly very important.

Initial calculations of authentication encumbrance and time behaviour are carried out to evaluate the authentication architectures for mesh networks. Symmetric grids of mesh stations stand for the mesh network, with a grid size of 3x3, 5x5 till 11x11 M-SS, including the M-BS in the centre of the grid. The M-BS symbolises the authentication server (M-AAA) of the mesh network. A two way handshake abstracts the basic authentication mechanism, such as access request of a supplicant and access replay from a authenticator. The RADIUS protocol [10] uses packet sizes from 20 to 4096 bytes to build authentication requests. The abstracted packet size, p-size, is selected to p-size = 100 byte per packet. Each delivery time, t-delivery, needed to transfer a packet between two mesh stations is supposed to t-delivery = 1 ms. The delivery time abstracts the characteristic of a connection between two mesh nodes. Mesh networks are wireless networks. Due to this fact, mesh network suffer under influences, such as reachability, interference and fairness of bandwidth distribution. Even if, these influences do not take place the connection characteristic depends on the routing mechanism. The behaviour of setting up a route, like proactive, e.g. optimised link state routing (OLSR), or reactive, e.g. ad-hoc on-demand distance vector (AODV), routing protocols, influences the time of transmitting a packet through the network. This behaviour is also comprised within the delivery time. Furthermore, each period of time needed to carry out an authentication process is derived to the authentication time, t-authentication, t-authentication = 40 ms. This stands for the mean time of a basic authentication request and answer; non-busy authentication server [11]. A computation time, t-computation, needed for M-SS internal processing, is set to t-computation = 1ms. Figure 3 presents the abstracted static authentication path with a grid size of 5x5 mesh stations as well as possible locations of the access decisions mechanisms.

Figure 4 depicts the authentication data behaviour of a mesh grid with a various amount of mesh nodes as supplicants. The static simulation model aims to present the proportional increasing of authentication data at a central authentication entity, like the M-AAA, depending on the amount of access requesting supplicants. Based on this result, it seems to be reasonable to insert more temporal authentication server within a mesh network architecture, e.g. used in a hierarchical or
distributed manner, to reduce the amount of authentication data at a central M-AAA server.

Fig. 3. Authentication path with a hop count of 3

The authentication time behaviour increasing by the hop count of mesh stations is depicted in Figure 5. It is a static simulation model, similar to the one depicted in Figure 3 and aims to present that the authentication time behaviour is influenced by the length of an authentication path and the hop count respectively. In this case the authentication time, t-authentication, focuses a single authentication request of a MN, no parallel authentication requests from other supplicants are considered. Beside the hop count, the authentication time arises from the transfer time, t-delivery, of a packet and the processing time, t-auth-process, of a authentication request within a AAA server. Moreover, the authentication time is influenced by the computation time, t-computation, of a packet within a M-SS. Figure 5 represents two extreme points, the minimum authentication time regarding a single authentication entity within the network and the maximum authentication time regarding a authentication entities within each M-SS. This behaviour allows an initial declaration. In the case of an initial authentication request of a MN the usage of a single authentication entity seems to be the efficient approach. The authentication time is smaller compared to the authentication time of the approach with a AAA-server within each M-SS. In this approach each M-SS has to carry out the authentication process, therefore the authentication time increases very much regarding the hop count of the authentication path. But regarding the authentication time in case of re-authentication a MN the AAA-server within the point of attachment seems to be a efficient approach. The authentication time is only affected by the single processing time of authentication and the delivery time of one hop. However, in the context of mobility, it is imaginable that a hybrid approach is beneficial. In this context, a hierarchical authentication approach comes up. The AAA information is stored more central compared to the distributed authentication approach, but stored more distributed compared to the central approach. Thus, the authentication time increases with the amount of additional hops between D-AAA and H-AAA server.

Fig. 4. Authentication data depending on the amount of supplicants

V. EVALUATION OF MESH AAA ARCHITECTURES

In summary, the location of access decision influences the authentication time behaviour in a significant manner. However, the selection of the location depends on the field of application, e.g. fixed or mobile access. With regard to fast initial authentication much authentication hierarchies seams to be unreasonable, because of the high authentication time. Concerning the authentication time of a MN within a train, the re-authentication time should be short a possible.

An initial evaluation of the architectures, such as central, hierarchical and distributed, considers the fundamental results mentioned in the previous section as well as characteristics of an applied network infrastructure, such as a wireless local area networks (WLANs). The transfer of the abstracted mesh network with a grid size of 11x11 mesh stations in a realistic environment, results in a mesh network coverage of 2200 m, using a radio cell range, r, with r = 100 m of a single MN. For example, a WLAN radio cell with a cell range of r = 100
m will be crossed by a moving vehicle with a speed of \( v = 100 \text{ km/h} \) (\( v = 200 \text{ km/h} \), \( v = 300 \text{ km/h} \)) in a period of time of 7.2 s (3.6 s, 2.4 s). In this case the moving node is connected to a M-SS for maximal 7.2 s (3.6 s, 2.4 s). In other words, a MN has to authenticate itself in the period of time of 7.2 s (3.6 s, 2.4 s).

Central approach: The centralised mesh authentication approach demands for least intelligence in the remaining mesh network infrastructure. On the other hand all authentication requests are forwarded through the whole mesh network to the M-AAA server (M-BS) for MN authorisation decision. Consequently, the bandwidth behaviour of the route changes. But at this stage of evaluation the amount of authentication data seems not to influence a broadband connection in a significant manner. Furthermore, the authentication time of MN increases depending on the length of the authentication path.

Hierarchical approach: The authentication decision is not carried out by a single authentication entity (M-AAA server). This approach avoids increased authentication data encumbrance within the mesh network, but demands more intelligence within the mesh network infrastructure compared to the central approach. Re-authentication of a MN is provided by the H-AAA server, while initial authentication of a MN is provided by the M-AAA server. In the case of non initial authentication, the authentication data and time is decreases compared to the central approach.

Distributed approach: The distributed approach reduces the authentication path length as well as the authentication data encumbrance to a minimum and provides the fastest way of re-authentication. On the other hand, the distributed approach demand for the most intelligence within the mesh network infrastructure.

Compared to the central and distributed architecture, the hierarchical architecture is the most suitable approach for mobility support. Due to the hierarchical distribution of AAA information the handover time behaviour between two neighbourd M-SS is shorter compared to the central and distributed approach. In both approaches a handover demands an initial authentication process that stay together with interaction of the M-SS with the M-AAA server. However, regarding the hierarchical approach the access request from the M-SS is send only to the H-AAA server. Concerning real time traffic, such as voice over IP (VoIP), a central or hierarchical authentication architecture should be able to fulfil the requirements of VoIP [12]. VoIP traffic demands connections with a delay smaller than 150 ms, to be emotionally sensed as uninterrupted by a user. As a result, to improve the seamless handover for real time traffic novel authentication mechanisms are needed to reduce the handover time. Suitable approaches could be pre-authentication or delayed-authentication of MN’s. In the context of location based service support the distributed architecture seems to be a suitable approach while the central architecture seems to support fixed and nomadic access in a suitable manner.

The static results are not sufficient enough to evaluate the authentication data and time behaviour in more detail. Further investigations for wireless mesh networks need the implementation of the three authentication architectures in the network simulator 2 (ns-2). The simulation results should be able to present the authentication data distribution within a mesh network and the authentication time behaviour regarding access request from many supplicant in parallel.

VI. CONCLUSION

This paper presents AAA requirements to provide carrier grade and railway grade mesh networks and investigates the authentication behaviour in wireless mesh networks. Three authentication architectures, such as central, hierarchical and distributed, for mesh networks are described. The results of the initial authentication data and time behaviour simulation are discussed in general and regarding different access scenarios, e.g. fixed, nomadic and mobile access. The most challenging access scenario, mobile access, seems to be best supported by a hierarchical authentication architecture, as this architecture provides the fastest handover behaviour. However, each concept has a justification in the context of a suitable access scenario. With regard to authentication times that support uninterrupted handovers for real time traffic, as VoIP, novel authentication concepts, such as pre-authentication or delayed-authentication, are able to enhance the handover behaviour.

REFERENCES