Authentication and Authorisation Mechanisms in support of Secure Access to WMN Resources

Markus Anwander, Torsten Braun, Almerima Jamakovic and Thomas Staub
CDS | IAM | University of Bern
Bern, Switzerland
anwander|braun|jamakovic|staub@iam.unibe.ch

***Abstract*—Over the past several years, a number of design approaches in wireless mesh networks have been introduced to support the deployment of wireless mesh networks (WMNs). We introduce a novel wireless mesh architecture that supports authentication and authorisation functionalities, giving the possibility of a seamless WMN integration into the home's organization authentication and authorisation infrastructure. First, we introduce a novel authentication and authorisation mechanism for wireless mesh nodes. The mechanism is designed upon an existing federated access control approach, i.e. the AAI infrastructure that is using just the credentials at the user's home organization in a federation. Second, we demonstrate how authentication and authorisation for end users is implemented by using an existing web-based captive portal approach. Finally, we observe the difference between the two and explain in detail the process flow of authorized access to network resources in wireless mesh networks. The goal of our wireless mesh architecture is to enable easy broadband network access to researchers at remote locations, giving them additional advantage of a secure access to their measurements, irrespective of their location. It also provides an important basis for the real-life deployment of wireless mesh networks for the support of environmental research.**

***Keywords*-wireless mesh networks (WMNs); authentication and authorisation infrastructure (AAI);**

I. Introduction

Wireless mesh networks (WMNs) are a candidate technology for providing a cost-efficient and user-friendly connection of remote sites to public or corporate networks. Besides these costs- and the usage-related benefits, wireless mesh networks include, as result of their mesh nature, the properties of a robust and self-managed network. For the mentioned aspects of their heterogeneous network design, WMNs are seen as an integration of two planes: the access plane provides connectivity to the end users while the forwarding plane relays traffic between the nodes connected with the mesh. Design of a wireless mesh network has also become more and more popular due to the increasing usage of multiple radios and (virtual) wireless interfacing techniques. Most current deployments are based on the IEEE 802.11 standard, however this by no means restricts the WMNs applicability to other standards, but availability of cheap IEEE 802.11 hardware has mostly motivated this growth. Because the IEEE 802.11 protocol stack was originally designed for infrastructure WLANs, various modifications are necessary when using it in WMNs. Other standards like WiMAX and 3G/4G are emerging and the knowledge gained by research and development of WMNs over 802.11 is likely to be very useful in the future deployment of these diverse scenarios.

There is a diverse range of possible application scenarios for wireless mesh networks. However, WMNs have enjoyed so far only limited deployment and were mainly used in community networks to provide cheap Internet access, in industrial settings for control and monitoring, and in military applications to enable mobile communications of field units. In the near future several new applications, mainly in the area of higher education and healthcare, are likely to make WMNs an everyday reality. In this paper we present a wireless mesh architecture to support secure broadband network access for researchers in remote areas. In particular, we present a novel authentication and authorisation mechanism, fully functional in WMNs, enabling authorized usage of network resources: the network resources can only be accessed by authenticated and authorized end users and machines. The WMN architecture is fully compatible with the existing AAI Shibboleth-based federation, such as SWITCHaai which is operated by SWITCH, the Swiss National Research and Education Network (NREN) operator. It is also compatible to other Shibboleth-based federations, e.g. Finland, Germany, US, etc. by only creating the appropriate attribute mappings. The WMN architecture provides a unique solution for authentication and authorisation of both end users and mesh nodes of a WMN. In addition, our solution may offer detailed accounting to enable further cost-sharing among different organizations and infrastructure-auditing. A development of a wireless mesh network architecture using authentication and authorisation mechanisms proved its value for the institutions of higher education as researchers from different areas, like climate research, geology, etc., may profit from an easily accessible and highly secure wireless mesh network, irrespective of their location.

The remainder of this paper is organized as follows. Section II gives an overview of previous design efforts regarding authentication and authorisation mechanisms in the WMN community. Section III introduces the wireless mesh network architecture that supports authentication and authorisation of end users and mesh nodes. Section IV explains a possible deployment of this WMN architecture for the purpose of environmental research. Section V

978-1-4673-1239-4/12/$31.00

summarizes our main results on the WMN authentication and authorisation mechanism and states several interesting problems for further research.

II. Related work

There has been quite some interest in the last few years in the design and deployment of wireless mesh networks. This is mainly due to the fact that WMNs imply both the ad-hoc network as well as the more traditional infrastructure model of access networks, posing various challenges for researchers and developers. A basic overview of the main research challenges in wireless mesh networks is provided in [1], and the most recent one in [2].

Generally, a WMN consists of wireless mesh nodes, which can operate as hosts but also as routers, being in this way access point for the mesh network. The mesh nodes are typically fully functional computers with tailored embedded operating systems so as to match hardware resource constraints. The mesh clients are often laptops, cell phones and other wireless devices, though often various measurement devices like sensors can be connected, either cabled or through a wireless link to a monitoring platform via a multi-hop connection of mesh nodes. Data generated by the mesh clients is forwarded from nearby mesh node to other peer mesh nodes (towards the destination) that are too far to reach in a single hop. The nodes' relatively stable connectivity (i.e. mesh topology) is also used for the exchange of management and configuration information. The basic requirement of forwarding end user data as well as the dissemination of network management data requires that the mesh nodes trust each other. This is one of the most important open questions that we solved by proposing a novel authentication and authorisation mechanism, tailored for the wireless mesh network supporting secure access to the network resources through a Shibboleth-based AAI infrastructure, in our case the one for Swiss institutions of higher education SWITCHaai [5].

An increasing number of the current secure IP-based service access solutions in European NRENs are based on federated identity-based authentication and authorisation infrastructures that support easy and secure inter-organizational access to network resources. With the identity-based concept an end user registers only once with his/her home organization and gets access to all network resources that are part of the federated identity-based system, referred to as Identity Management (IdM) system. In Federated IdM system, federated refers to the fact that an end user identity and attributes are stored across multiple distinct identity management systems. A well-known example of federated IdM is the eduroam (education roaming) service [6] and at smaller national level e.g. SWITCHaai, facilitating network access to attendees from participating institutions of higher education. Eduroam is based on a RADIUS [3] infrastructure with IEEE802.1X [7] whereas SWITCHaai [5] on a Shibboleth Federated Identity Management system [4]. The former one requires federation of Remote Authentication Dial-In User Service (RADIUS) servers that facilitate network access to roaming academic affiliates using IEEE820.1x as the vehicle. We describe briefly how in general terms the authentication and authorisation has been designed by RADIUS.

First, an end user sends a request to the controlling-access-to-network gateway (being generally some kind of remote access server), to gain access to a particular network resource using access credentials. Typically, the access credentials are saved in the form of a username and password, or a certificate provided by the end user. In turn, the gateway sends to the RADIUS server a RADIUS access request (using RADIUS protocol), which includes credentials, requesting authorisation of the end user. The RADIUS server checks whether this information is correct and returns a proper response to the gateway, which in turn grants access to the end user. The latter example of federated IdM system, i.e. SWITCHaai, is based on Shibboleth architecture and allows implementation of an Authentication Authorisation Infrastructure (AAI) mechanisms especially designed to protect web services. The conceptual difference with the previous example is that the Shibboleth architecture involves an end user sending a request to the controlling entity, which here is a Service Provider who in turn redirects the end user's request to the home's organization Identity Provider (IdP). The home's organization IdP consecutively approves a request and redirects the end user once again to the Service Provider being responsible to authorize the end user. SWITCHaai changes this architecture in the way that the IdP directly talks to the controlling entity being here a web-based access point. The access point sends afterwards a request for permissions to the authorisation server and if the request is granted, the firewall is opened to allow full access to the Internet.

From the two examples, we may conclude that the majority of the approaches for secure IP-based service access are based on federated identity-based approach, and involve authentication and authorisation of end users only. Although, there is substantial literature and expertise on the end user-based identity verification techniques, hardly any attention has been paid on the process of authentication and authorisation of machines, especially in a community WMN context. Several contributions like [8]–[11] pinpoint the need and give partial solutions, however to this day there is a little understanding of the authentication and authorisation design in WMNs as a whole, especially during an occasional failure or addition of new mesh nodes. In this respect, by introducing a novel approach for the machine authentication and authorisation in WMNs we make an important step in deploying a fully functional WMN for supporting researcher requirements of higher education institutions.

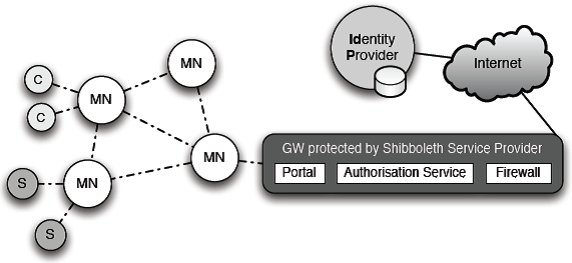

Figure 1. Schematic representation of the authentication and authorisation mechanism.

III. Authentication and Authorisation Mechanisms in WMNs

The developed WMN architecture supports basic security functionalities, namely authentication, and authorisation. The goal of the authentication and authorisation functionality is to prevent unauthorized usage of network resources. Only authenticated and authorized end users may get access to the network. In addition, only authenticated and authorized mesh nodes can join the WMN. Whereas the network access for end users can be performed by existing approaches such as IEEE 802.11x / RADIUS used in eduroam or a web-based captive portal protected by SWITCHaai, new approaches are necessary for machine authentication and authorisation in WMNs.

Our proposed mechanisms for authentication and authorisation works as follows (see Figure 1). The A^4-Mesh network implements two (virtual) wireless networks, an unencrypted one for joining the network and an encrypted one for data communication. Per default, the A^4-Mesh network allows for only unencrypted connections for joining the network and encrypted connections for full access to the mesh network and the Internet. The unencrypted mesh network only forwards traffic necessary for authentication and authorisation towards the gateway. All other traffic is blocked and discarded by the firewall of the gateway. The gateway serves as the main controlling entity, and for that it uses the AAI federation based on Shibboleth architecture: Once again, it involves an end user sending a request to the controlling entity, which here is a Service Provider, located on the gateway, who in turn redirects the end user's request to the home's organization IdP, which consecutively approves a request and redirects the end user once again to the Service Provider being responsible to authorize the end user. After successful authentication, additional attributes stored at the IdP are transmitted to the gateway for authorisation.

For end user authentication, the existing SWITCHaai federation is used so as to authenticate end users that want to join the mesh network, but also to protect the mesh network administration web-interfaces. For machine authentication a separate Shibboleth federation is used. The IdPs of this separate machine federation use X.509 client certificates instead of user password credentials for authenticating mesh nodes at the IdP. As Shibboleth perfectly handles multi-federation setups, this solution can be easily integrated into the existing AAI Shibboleth-based federation, operated by SWITCH.

A. End user authentication and authorisation scheme

First, the end user authentication and authorisation procedure is depicted in Figure 2. The main components of the system are the mesh nodes (MN), the mesh network gateway (GW) and an end user with its mobile device. A mesh node (MN) acts, in addition to providing the mesh interconnection links, as a wireless access point offering end users a public wireless network and hence wireless high speed access to the Internet. An end user can join this network using its mobile device. The dynamic Host Configuration Protocol (DHCP) server located on each MN assigns an IP address to a joining end user's mobile device. Primarily, after having joined the public network, a new mobile device does not get access to the Internet and instead all its traffic is blocked by a firewall on the local MN.

For each mobile device, an end user has to get authenticated and authorized before gaining full network access. This procedure is based on a captive portal solution, If the end user tries to access a web page, his/her first http request is forwarded by the captive portal component of the MN to the central captive portal service on the mesh network gateway. Depending on the availability of public IP addresses, the A^4-Mesh network may use either public addresses for clients or introducing network address translation (NAT) at the mesh nodes. In any case, the forwarded user request always contains the IP address of the MN as well as the IP address that has been allocated to the mobile device. The central captive portal service is a Shibboleth service provider, in our case part of the SWITCHaai Shibboleth federation. Being redirected to the Shibboleth protected captive portal web page, the end user has to perform a standard Shibboleth authentication. He/she gets redirected

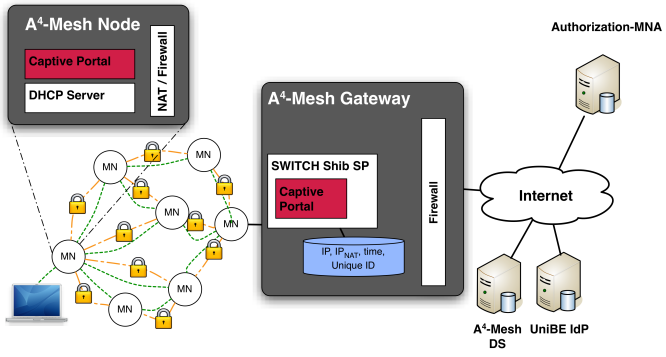

Figure 2. End user authentication and authorisation scheme based on captive portal.

to the IdP of the home's organization that he/she has selected from the discovery service (SWITCHaai-DS). In our example, it is IdP of the University of Bern (UniBE). After successful authentication, the captive portal uses the received SWITCHaai end user attributes to perform an authorisation request at the authorisation service. Authorisation service may in addition provide authorisation for end users based on groups/roles they belong to. If network access is authorized, the captive portal opens the firewalls at the MN and the gateway for the mobile device. Moreover, it logs the end user IP address (IP_{NAT}), mesh node IP address, time and unique identifier from Shibboleth for the accounting system. In order to keep track of the authorized end users, the captive portal cuts the networks access for a mobile device after a predefined period of time by blocking the firewalls and requires repeating the authentication and authorisation procedure.

B. Machine authentication and authorisation scheme

The machine authentication and authorisation procedure is depicted in Figure 3. The main components of the system are the mesh nodes (MN), the gateway (GW), the Mesh Node Authorisation (MNA), and the Machine IdP. The mesh nodes interconnect to form a wireless mesh network, establishing two different networks, a public and an encrypted network. In order to access the Internet or an Intranet, the MNs have to communicate over the encrypted network. General network access is blocked for the public unencrypted network, i.e. only certain IP addresses (Gateway, MNA, DS, and IdPs) are reachable over the public network. It only serves as entry point to get authorisation for the encrypted network. The authentication and authorisation sequence diagram is depicted in Figure 4. The authentication/authorisation agent of a MN that wishes to join, requests the key for the encrypted network from the AA-portal through the public network. Upon this request, the portal redirects the node to the corresponding machine authentication IdP, which authenticates the mesh node by an X.509 certificate and replies with a reference to an authentication assertion.

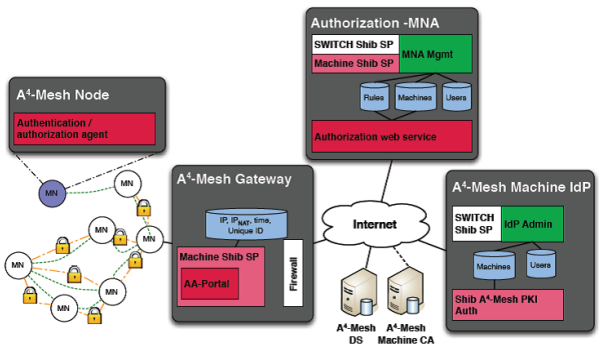

Figure 3. Our proposed mechanism for authentication and authorisation of mesh nodes in WMNs.

Using this reference, the AA portal on the GW requests the attributes from the IdP (e.g., the unique identifier of the machine). Using these attributes, the portal can check the authorisation of the mesh node at the Authorisation service. After successful authentication and authorisation, the gateway conveys the network key to the mesh node, thus allowing the traffic from and to the mesh node through its firewall. It also keeps track of the process and writes the IP address, time and unique identifier of the mesh node to a database for the accounting system. Finally, the mesh node joins the encrypted network with the received key and is then fully integrated in the WMN. A mesh node connects every 30 minutes to the AA-Portal to renew the authentication and provide a keep-alive information for the firewall and accounting system.

If a (new) joining mesh node is unknown to the Authorisation service, the gateway forwards the mesh node to the MNA Management entity for joining the network. The MNA Management provides a functionality of a mesh node subscription service. It is protected by a Shibboleth Service Provider, which belongs to the mesh network federation: it retrieves the Shibboleth attributes of the MN (e.g. unique identifier). This federation is referred to as Machine Shibboleth federation, solely introduced for machine authentication. The MNA Management mesh node subscription service uses these attributes from the IdP to initiate a node subscription for network access. A notification message is sent to the responsible administrator, which can confirm or deny the subscription to his network. Furthermore, the MNA Management as well as the machine IdP and AA-Portal are using a special authentication language based on XML-tags, which enables the receiving entity to easily distinguish between several received answers. The AA-Portal, after receiving the response to an authorisation request for a unique ID, can now easily distinguish between several answers from MNA Management, i.e. no-subscription and machine-unknown-to-MNA, in case this unique ID has no subscription yet or it is unknown to the MNA database. In both cases, the AA-Portal forwards the mesh node to the MNA Management subscription page from which several possible answers are given back to the AA-Portal and in turn to the authentication/authorisation agent of a MN. Those answers are: machine-authorized, subscription-pending, machine-suspended and machine-rejected. The advantages of XML status messages are both machine and human readable and interpretation, and easy integration in of-the-shell IdP.

System administration with the web-based access to the MNA Management entity is protected by a SWITCHaai Shibboleth Service Provider: Administrators have to be authenticated and authorized before accessing the web-based network management and monitoring of the mesh network. In order to be easily adoptable to the current SWITCHaai policies and contracts, allowing only accounts for end users,

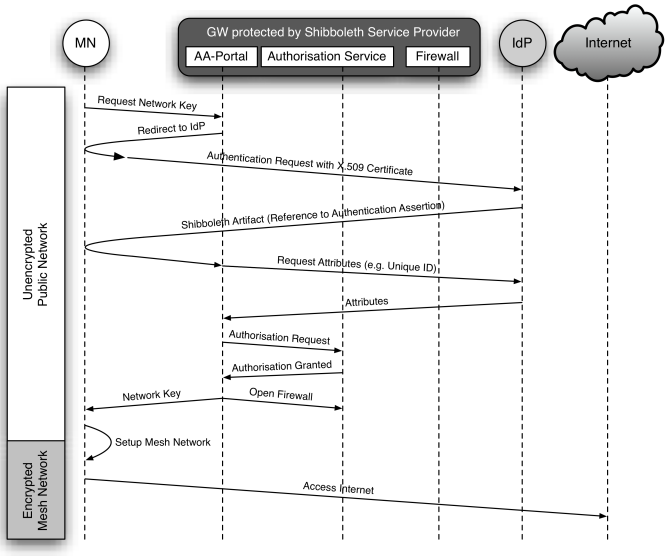

Figure 4. Sequence diagram for authentication and authorisation of mesh nodes.

the regular SWITCHaai federation is used to authenticate network administrators for the machine identity management at the machine IdP, and for authorisation management at the MNA Management. A new separate Shibboleth federation is solely used for machine authentication. As Shibboleth perfectly handles multi-federation setups, this solution can be easily implemented.

IV. A^4-Mesh Network For Supporting Enviromental Reserach Requirements

There is a diverse range of possible application scenarios for the deployment of wireless mesh networks. Our application scenario considers an extensive hydro-meteorological monitoring network that has been set up for estimating and modeling water availability under present and future conditions. This hydro-meteorological monitoring network consists of different measurement devices and these all produce large amount of data, which needs to be transferred from the different remote sites to the university campus, preferably in near real time. For researchers it would be very convenient and desirable to directly access measurement devices from a campus site, ensuring in this way data transfer at frequent intervals as well as the option of remote control, which both reduces the risk of data loss by the sensors, e.g. in case of memory overruns. A wireless communication mesh network serves accordingly the purpose of a (temporary) measurement infrastructure, giving researchers low-cost broadband network access in virtually any remote area. Since one of the goals of A^4-Mesh was to allow end users with a non-technical background to deploy mesh nodes to extend a campus network, special care has been taken regarding seamless integration of authentication and authorisation functionalities into the organization's own authentication and authorisation infrastructure. Moreover, deployment of real wireless networks requires careful design and meticulous consideration of various hardware/software/technology aspects without which the network performance can be poor or even erroneous. Accordingly, the deployment of A^4-Mesh will proceed in steps with the strong argument for considering different parameters, related to environment, planning, etc.

The current setup of the envisioned wireless mesh network consists of seven wireless mesh nodes interconnecting the hydrological sensors to the university campus network. Figure 5 shows the current setup with the distances of each wireless link along with the locations of the connected environmental monitoring stations. The network deployed in the Swiss alps is a common form of WMNs where every mesh node relayS data for other mesh nodes (a typical ad-hoc networking paradigm), and given mesh routers also have the additional capability of being Internet gateways. Node 1 serves as a gateway to the fixed network backbone. In this way it carries the traffic between the mesh nodes and the Internet. The first link from node 1 is directed to a relay station (node 2) in Vercorin at the opposite hill slope, where a webcam is located. The second link from node 1 connects to nodes 4b and 4a in Cry d'Er, which in turn interlink with all the other nodes except node 3. Clients, i.e. measurements stations, connect to these routers using wireless or wired links. The incremental addition of nodes is the following step in the network deployment, extending the network with two additional mesh nodes.

The region where the mesh network is deployed has extreme weather conditions with a lot of snow in the winter, requiring mesh nodes that are specifically built for these conditions, i.e. durable cases, self-contained power supply based on a solar panel at least 3 meters above the ground to prevent them from being covered by snow and batteries powerful enough in case of poor sunlight. Additionally, as a way to improve lifetime and reduce maintenance cost of WMNs, most of the mesh nodes (those that are covered by the cellular networks) have a backup mesh node with UMTS. In the case that an erroneous image gets uploaded to a mesh node, we are able to connect to the UMTS mesh node and reboot the node, or upload a new image instead of physically accessing the node. Finally, the current deployment of the A^4-Mesh wireless mesh network is based on the IEEE 802.11n standard, which builds on previous 802.11 standards by adding multiple input multiple output (MIMO) technology to improve the network throughput between neighboring stations. This by no means restricts this WMNs' applicability to other standards but cheap availability of IEEE802.11 WLAN hardware has mostly motivated this choice. We have set up a basic installation of the wireless network for environmental research but the deployment issues showed that further work is still needed.

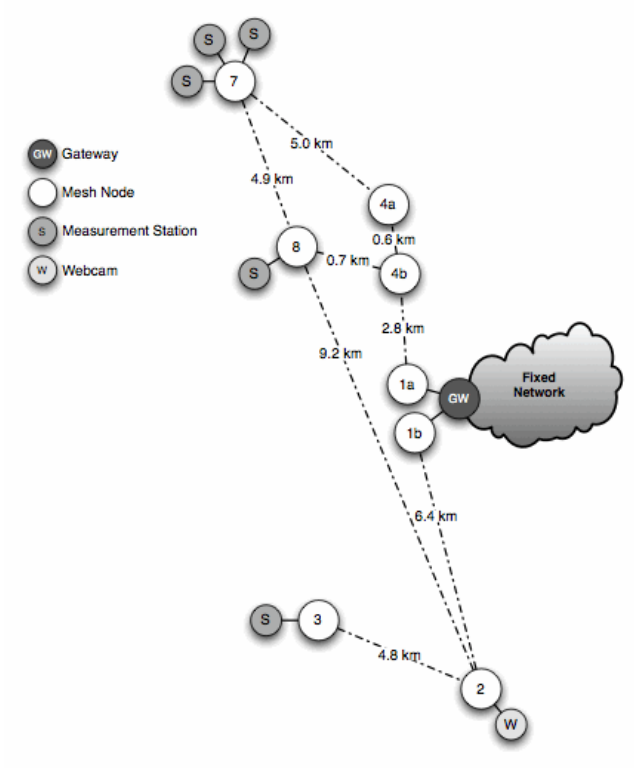

Figure 5. Current setup of the wireless mesh network for environmental research.

V. Conclusion and Further Work

In this paper we have introduced a novel authentication and authorisation mechanism to be used in WMNs when end users and mesh nodes want to make use of the network resources: only authenticated and authorized end users may get access to the network, and only authenticated and authorized mesh nodes can join the WMN. Generally, we looked at the ways how to create value for researchers giving them easy and secure access to a wireless mesh network (and their measurements), irrespective of their location. As a result we presented a new approach for the mesh node authentication and authorisation in WMNs. For the access to network resources by end users, we adapt a web-based captive portal approach. Both mechanism for authentication and authorisation in WMNs are furthermore fully compatible with the existing AAI Shibboleth-based federation, SWITCHaai, deployed by the Swiss NREN SWITCH. In this paper, furthermore, we have focussed on the deployment of the end user and mesh node authentication and authorisation mechanisms in an environmental monitoring scenario in the Swiss Alps. There are several challenges and problems we encountered during the deployment, and they all deal with the aspects of usable and sustainable deployment of real outdoor wireless mesh networks. Hence further work is required on sustainable WMN implementation and deployment, taking into account all the other design objectives that affect the performance of WMNs when deploying a real wireless mesh network.

Acknowledgment

The A^4-Mesh project is carried out as part of the program "AAA/SWITCH - e-Infrastructure for e-Science" lead by SWITCH, the Swiss National Research and Education Network, and is supported by funds from the Swiss State Secretariat for Education and Research.

References

[1] H. Moustafa, U. Javaid, D.E. Meddour, and S.M. Senouci, *A Panorama of Wireless Mesh Networks: Architecture, Application and Technical Challenges*, Proc. of International Workshop on Wireless Mesh: Moving towards Applications (Wimeshnets 06), 2006.

[2] P.H. Pathak and R. Dutta, *A Survey of Network Design Problems and Joint Design Approcahes in Wireless Mesh Networks*, IEEE Communications Surveys & Tutorials, vol. 13, no. 3, 2011.

[3] C. Rigney, S. Willens, A. Rubens, and W. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, Internet Engineering Task Force, RFC 2865.

[4] S. Carmody, et al, *Shibboleth Architecture: Protocols and Profiles*, Internet2, Architecture Specs, September 2005.

[5] C. Graf, et al, *AAI - Authentication and Authorisation Infrastructure System and Interface Specification*, SWITCH, System Specs, January 2004.

[6] M. Milinovic, et al, *Eduroam: Service Definition and Implementation Plan*, GEANT2, Deliverable DS5.1.1, July 2008.

[7] B. Aboba, et al, *Extensible Authentication Protocol (EAP)*, Internet Engineering Task Force, RFC 3748, June 2004.

[8] K. Khan and M. Akbar, *Authentication in Multi-hop Wireless Mesh Networks*, 16th Inter. Conference on Computer Science and Engineering (CISE 2006), 2006.

[9] O. Cheikhrouhou, M. Laurent-Maknavicius, and H. Chaouchi, *Security Architecture in a Multi-hop Mesh Network*, Proc. of the 5th Conference on Security and Network Architectures (SAR 06), 2006.

[10] F. Martignon, S. Paris, and A. Capone, *Mobisec: A Novel Security Architecture for Wireless Mesh Networks*, Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks (Q2SWinet 08), 2008.

[11] M. Manulis, *Securing Remote Access Inside Wireless Mesh Networks*, Information Security Applications: 10th International Workshop (WISA 2009), 2009.