Operational Support of Wireless Mesh Networks Deployed for Extending Network Connectivity

T. Staub, B. Nyffenegger, D. C. Dimitrova, and T. Braun

staub|nyffenegger|dimitrova|braun@iam.unibe.ch
IAM, University of Bern, Switzerland

Abstract. Wireless mesh networks (WMNs) have shown high potential to extend the coverage of high bandwidth infrastructure networks. We propose a deployment of a WMN for the needs of higher education institutes. In order to provide extended coverage to campus networks, several open issues such as authentication and authorisation of connected nodes, accounting of network usage and auditing of the network, have to be addressed. This paper outlines our proposal and its relevance in practice and discusses how we intend to solve the mentioned issues.

1 Introduction

Wireless mesh networks (WMNs) have been around for several years as a wireless paradigm between infrastructure networks and ad-hoc networks. Generally, a WMN consists of wireless mesh nodes, which can operate as hosts but also as routers, i.e., working as access points for the mesh network. The mesh nodes are typically fully functional computers with tailored operating systems to match hardware resource constraints. Data is forwarded from node to node towards its destination. The nodes' connectivity is also used for the exchange of management and configuration information. User data forwarding as well as management data dissemination requires that mesh nodes trust each other. Hence, one of the challenges in WMNs is the provisioning of appropriate authentication and authorisation mechanisms. A basic overview of the main research challenges in wireless mesh networks is provided in [5].

WMNs provide efficient, scalable means to offer service coverage to a large number of users with different communication needs [1]. They can complement existing high bandwidth networks and connect devices at remote locations. Since its introduction, WMNs have shown high potential for practical deployment and significant commercial impact. For example, after a successful prototype launch at the Massachusetts Institute of Technology and a pilot deployment in London, Nortel proceeded to deploy commercial networks in, among others, the city of Taipei (Taiwan), the Kennedy Space Center (US) and Edith Cowan University (Australia) [6]. Cisco Systems has also released their own Outdoor Wireless Network Solution[1] as the means to support mission-critical business applications. Their proposal to ensure outdoor wireless security is described in a white paper

[1] Consulted in March 2011 at `http://www.cisco.com/en/US/products`

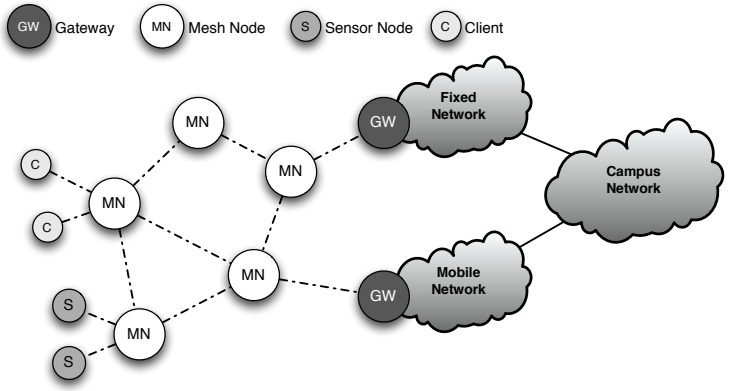

Fig. 1. General composition of a mesh network.

released by CISCO on their web-site[2].
Following the experience of others, we propose to use a WMN to supplement an existing university campus fixed network infrastructure with additional wireless coverage. Our goals are to develop, deploy and test a fully functional WMN tailored to the needs of the Swiss institutes of higher education. The proposed network deployment is illustrated in Figure 1. A WMN offers remote users, e.g. notebooks, access to the campus network. The WMN uses dedicated gateways to connect to a network with high bandwidth capacity, e.g., a fixed infrastructure network or a mobile network, which are also connected to the campus network. We propose a fixed infrastructure network as the broadband backbone mainly for two application scenarios, i.e. the extension of a campus network and the connection of remote areas for field experiments.
For an operational network, several requirements have to be met, namely the support of authentication, authorisation, accounting, and auditing (altogether referred to as A4). Authentication and authorisation control the access to the network. Accounting mechanisms enable the correct association of a service to a particular user and perform charging. Auditing should be in place to assist the undisturbed operation of the network by constant monitoring for abnormal behaviour.
The remainder of the paper is organised as follows. First, in Section 2 we address the practical relevance of the research and, in our opinion, its most probable impact areas. Next, Section 3 introduces the A4 functionalities and how we intend to realise their support by the proposed network scenario. Finally, in Section 4 we discuss several challenges that need to be faced and the future steps ahead of the project.

[2] Available in March 2011 at `http://www.cisco.com/en/US/solutions`

2 Practical Relevance

In this section we first describe what are potential applications of the envisioned wireless mesh network. The specifics of the application scenarios partly determine the requirements set towards the WMN. Next, we discuss the expected impact of the proposed research for both practical deployment and scientific contribution.

2.1 Application Scenarios

In our effort to enhance a WMN with the functionalities from Section 3 we are guided by its deployment for two main applications - extending coverage of campus networks and enabling of monitoring in remote areas. We now continue to describe both scenarios in more detail.

WMNs can complement the fixed Internet network in order to extend wireless network coverage in university campus networks. This does not only support individual students and employees in their work but also offers more freedom in organising group activities such as project meetings or educational fairs. To successfully use wireless mesh networks in the area of the Swiss higher education, WMNs have to support authentication, authorisation, accounting, and auditing. Since a campus network belongs to a particular university, access to the network should be provided only to authorised users. Hence, the WMN needs to support authentication and authorisation. As there are usually multiple concurrent users of the network, accounting is necessary in order to enable appropriate billing of the costs to the different users. Last but not least, for a successful operation of a WMN, inconsistent and erroneous states in the network have to be detected and resolved. This requires constant auditing of the network state and configuration such that alarms are triggered or even self-healing can be performed.

In the area of environmental monitoring applications, we distinguish several cases in which wireless mesh networks can provide additional connectivity. In all these monitoring scenarios, the sensor nodes are generally located in remote areas without access to a high bandwidth network infrastructure. In such situations, deploying a wireless mesh network provides a cost-efficient solution to connect these devices to the fixed network infrastructure. Remote environmental monitoring, e.g., related to glaciers, avalanches or landslips, is an intuitive candidate for the deployment of WMNs as cellular networks are not always available or have limited bandwidth. Another excellent candidate is agricultural monitoring, which is often associated with gathering information on soil humidity, precipitation and solar radiation over vast geographical areas. Deployment of a fixed network infrastructure over these areas is not reasonable. However, the collected sensor data still needs to be accessible. Another possibility is the deployment for weather monitoring, in which case the weather/climate monitoring stations need to communicate their collected data to a centralised entity in order to enable, e.g., weather forecasting.

Aside of the two main deployment scenarios described above, WMNs can be used to enable other outdoor monitoring and surveillance applications such as

surveillance of restricted areas and service provision for research events of limited duration.

2.2 Expected Impact

We identify two perspectives from which the proposed study is beneficial for the development in wireless mesh networks.
First, the practical point of view is clearly important. The results can be used to extend campus network coverage (in the order of kilometres) by universities. WMNs may further be used for temporarily deployed network services for events and research projects, e.g., excursions and outdoor research experiments. Further, research initiatives in various research areas (climate research, geology and biology) may profit from an easily deployable outdoor wireless network that supports high speed network access as well as authentication, authorisation, accounting, and auditing. The latter two functionalities, i.e., accounting and auditing, are particularly attractive. The ability to charge independent parties enables the concurrent use of the wireless network infrastructure by multiple projects; auditing functions increase awareness on network health and reduce network maintenance costs. In conclusion, we believe that the proposed research has a high potential for providing the basis for commercial WMN services.
Second, there is the scientific value of the research. We intend to provide not only a theoretically sound solution but also a practically feasible one. Hence, the developed mechanisms will consider many practical details and constraints and will be very well suited for deployment.

3 The A4 Concept

This section presents the four basic functionalities - authentication, authorisation, accounting and auditing - required by the WMN in our proposed A4-Mesh network. We also discuss the envisioned architecture, which we have just defined at the present stage of the research, to support these functionalities. However, there are still several options open to explore and as result this initial architecture might undergo redesign. In addition, we expect certain changes may be necessary as a result of future design insights or unforeseen deployment issues.

3.1 Authentication and Authorisation

The goal of the authentication and authorisation functionality is to prevent the unauthorised usage of the network resources. Only authenticated and authorised users and sensors get access to the network. In addition, only authenticated and authorised mesh nodes can join and be part of the WMN. Whereas the network access for end users can be performed by existing approaches such as IEEE 802.11x / RADIUS used in eduroam[3] or a web-based captive portal protected

[3] www.eduroam.org

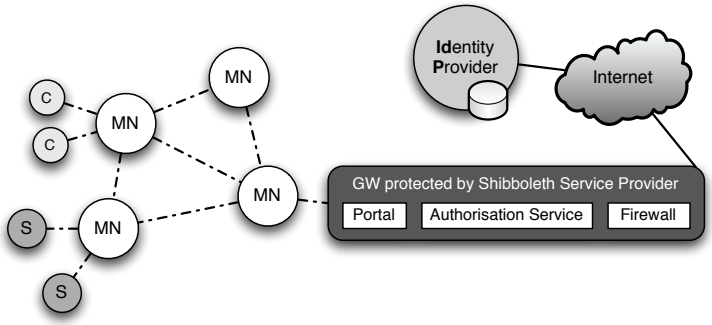

Fig. 2. Schematic representation of the authentication and authorisation mechanism.

by SWITCHaai[4], new approaches are necessary for machine authentication and authorisation.

Our concept for machine authentication and authorisation is as follows. The A4-Mesh network implements two (virtual) wireless networks - an unencrypted one for joining the network and an encrypted one for data communication. Per default the A4-Mesh network just allows 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 the necessary traffic for authentication and authorisation towards the gateway and the Shibboleth Identity Provider (IdP). All other traffic is blocked by the firewall of the gateway. The mesh nodes can get authenticated by the IdP through credentials or certificates. After successful authentication, additional attributes stored at the IdP are transmitted to the gateway for authorisation. For the machine authentication we intend to set up an additional IdP within the SWITCHaai Shibboleth federation to have the full flexibility of supporting different attributes for the mesh nodes than for normal SWITCHaai users. For user authentication, the existing IdPs are used.

The machine authentication and authorisation procedure is depicted in Figure 2. A joining mesh node (MN) first requests the key for the encrypted network from the 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 a X.509 certificate and replies with a reference to an authentication assertion. Using this reference, the portal on the gateway (GW) requests the attributes from the IdP (e.g. the unique identifier). 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 and thus allows traffic from and to the mesh node through its firewall. Finally, the mesh node joins the encrypted network with the received key and is now fully integrated in the WMN.

[4] www.switch.ch/aai

In addition, administrators have to be authenticated and authorised before accessing the web-based network management and monitoring of A4-Mesh. The network management therefore uses the Shibboleth service provider for user authentication. Based on the authentication, the network management handles the authorisation.

3.2 Accounting

As accounting, we define the ability to collect and store network-related information for later use. A WMN requires an accounting solution for various reasons such as charging users, network planning or increasing the network performance. To charge individual users for the network usage, the induced traffic of these users must be measured and network statistics may be used for network planning purposes. Finally, a WMN can provide similar characteristics as fixed networks in terms of robustness and reliability. This can be achieved by measuring the traffic on the individual links and exploiting multi-path, multi-channel and multi-interface routing mechanisms, inherent to wireless mesh networks. Path selection procedures are based on Quality of Service (QoS) characteristics such as available bandwidth, experienced bit and packet error rates and interference levels.
An accounting solution has to store the required information with the desired level of detail while simultaneously meeting resource constraints; in particular concerning storage capacities on mesh nodes. We therefore propose a distributed accounting architecture using short-term and long-term data and intend to incorporate parts of the AMAAIS (Accounting and Monitoring of AAI Services [7]) project which acts as an extension to SWITCHaai and provides mechanisms for

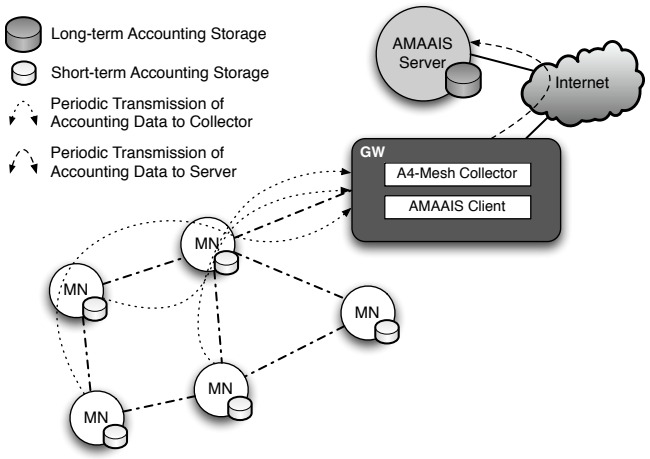

Fig. 3. Schematic representation of the accounting procedure.

accounting and monitoring. The architecture of the A4-Mesh accounting mechanism is depicted in Figure 3. The individual mesh nodes will gather short-term accounting data, which includes QoS characteristics of the neighbours and periodically transmit the information to the gateway. This data is also used to select the best communication channel for the transmission. The gateway processes the accounting data with a collector component and passes it on to the AMAAIS client which aggregates the short-term data and periodically transmits it to an AMAAIS server over the Internet. The AMAAIS server stores the long-term accounting data and enables billing of the costs, network dimensioning and planning.
Once available, the accounting data can be used for other purposes as well, such as the automation of path selections. Introducing intelligence locally in the nodes enables them to automatically choose a communication path fitting the needs of the transported data. To assist the selection process we intend to use a recommender system that considers both, the QoS characteristics offered by the network and the QoS characteristics required to transport the data. For example, if a path was able to successfully transport data with specific requirements (low delay, low jitter, low loss) under certain circumstances, it is possible that other paths with similar characteristics can be suitable as well. The benefits of such automated network (re-)dimensioning are reduced administrative overhead and a self-organised network.

3.3 Auditing

Audits are performed to ensure the validity and reliability of information; also to provide an assessment of a system's internal control. Due to (autonomic or manual) network management operations, as well as other external impacts, inconsistent or erroneous node states can occur. Examples for erroneous network states are the selection of frequencies that are not used by any neighbouring nodes or routing tables causing loops. One reason for service disruption can be the inappropriate choice of wireless radio or routing parameters due to, e.g., corrupt self-management mechanisms of the wireless mesh nodes. Another reason might arise from different versions of system software which may lead to compatibility problems and compromise interoperability of mesh nodes. The introduction of auditing functions should allow the detection of wrong and inconsistent configurations and report them to a network operator or perform an appropriate self-healing procedure.

4 Challenges and Further Development

Currently, we are working on building the mesh nodes, which will be used for an outdoor test bed. The outdoor test bed is situated in the region of Crans-Montana, Switzerland with some mesh nodes installed in remote areas. The region has harsh weather conditions with a lot of snow in the winter and requires mesh nodes specifically built for these conditions, i.e. durable cases, solar panels

at least 3 meters above ground to prevent them from being covered by snow or batteries large enough in case of poor sunlight. We are also adding a backup mesh node with UMTS access to some of the regular mesh nodes, which are covered by the cellular networks. In the case that an erroneous image gets uploaded to a mesh node, we will be able to connect to the UMTS mesh node and reboot the regular mesh node or upload a new image instead of physically accessing the node.
The next step is completing and testing the implementations of the specific A4-Mesh functionalities. Since one of the goals of A4 is to allow users with a non-technical background to deploy mesh nodes to extend a campus network, special care has to be taken in regard to ease of use and seamless integration in the organisation's own authentication and authorisation infrastructure.

Acknowledgements

The A4-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. I. F. Akyildiz, T. Melodia, and K. R. Chowdhury. A survey on wireless multimedia sensor networks. *Comput. Netw.*, 51:921–960, 2007.
2. E.R. Cruz, D. Camara, and H.C. Guardia. Providing billing support in wimax mesh networks. In *Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009. IEEE International Conference on*, pages 161 –166, 2009.
3. K. Khan and M. Akbar. Authentication in multi-hop wireless mesh networks. volume 16. 16th Intl. Conference on Computer Science and Engineering (CISE 2006), World Academy of Science, Engineerig and Technology, 2006.
4. Mark Manulis. Securing remote access inside wireless mesh networks. In Heung Youm and Moti Yung, editors, *Information Security Applications*, volume 5932 of *Lecture Notes in Computer Science*, pages 324–338. Springer Berlin / Heidelberg, 2009.
5. H. Moustafa, U. Javaid, D. E. Meddour, and S. M. Senouci. A panorama on wireless mesh networks: Architectures, applications and technical challenges. Proceedings of International Workshop on Wireless Mesh: Moving towards Applications (Wimeshnets '06), 2006.
6. S. Roch. Nortel's Wireless Mesh Network solution: pushing the boundaries of traditional WLAN technology. Notrel Technical Journal, 2005.
7. Burkhard Stiller. Accounting and Monitoring of AAI Services. *SWITCH Journal*, 2010(2):12–13, October 2010.