



Workshops der
Wissenschaftlichen Konferenz
Kommunikation in Verteilten Systemen 2009
(WowKiVS 2009)

A Secure Remote Authentication, Operation and Management
Infrastructure for Distributed Wireless Sensor Network Testbeds

Philipp Hurni, Thomas Staub, Gerald Wagenknecht, Markus Anwander, Torsten Braun

6 pages

A Secure Remote Authentication, Operation and Management Infrastructure for Distributed Wireless Sensor Network Testbeds

Philipp Hurni, Thomas Staub, Gerald Wagenknecht, Markus Anwander, Torsten Braun

Institute of Computer Science and Applied Mathematics
University of Bern, Switzerland
{hurni, staub, wagen, anwander, braun}@iam.unibe.ch

Abstract: In this paper we propose an infrastructure for a secure remote authentication, management and operation system for a distributed global wireless sensor network testbed. We base the design of the architecture on an existing well-established, widely deployed and frequently used authentication and authorization system developed to simplify inter-organizational access to web-resources. The proposed infrastructure addresses the main challenges of a interconnected distributed sensor network testbed, such as secure remote availability, multi-user access, confidentiality and integrity. The paper further describes our perspective of a testbed workflow management and operation system aiming to provide a simple and comprehensive interface for remote wireless sensor network configuration and experimentation.

Keywords: Wireless Sensor Networks Testbed Authentication and Management

1 Introduction

All over the world, universities have set up small wireless sensor network testbeds for research purposes, in order to test and evaluate own proposed mechanisms and to analyze and evaluate their real-world behaviour and characteristics. So far, a couple of testbeds have been put into operation, with different equipment and testbed design (e.g. MoteLab [WSW05], TutorNet [Tut], Kansei [AER⁺06]). However, a compound network to interconnect different wireless sensor network testbeds at different locations, offering access to networks in different environments, with heterogeneous hardware and operating systems, in analogy to Planetlab [BBC⁺04] for wired distributed systems in the Internet, is still missing.

The EU 7th Framework Programme project WISEBED [Wir] intends to bridge this gap. It aims to provide a multi-level infrastructure of interconnected testbeds of large-scale wireless sensor networks for research purposes. The project targets to interconnect wireless sensor testbed networks of heterogeneous small-scale devices, to simplify and automate remote network access, configuration, experimentation, extraction and evaluation of results. WISEBED intends to establish a compound network of heterogeneous sensor network testbeds - a network of wireless sensor networks. Researchers shall be enabled to run their recent developments of sensor network algorithms and mechanisms on different remote testbed sites. With universities sharing their wireless sensor network resources, researchers can test their algorithms and prototypes on different hardware without having to purchase new equipment. The available resources can

be used by more researchers, which in turn increases resource utilization and cost-efficiency. Furthermore, the availability of interconnected distributed sensor network laboratories allows running totally new kinds of experiments, e.g. with algorithms gathering and processing sensor data across the testbed boundaries.

2 Testbed Authentication and Authorization using Shibboleth

An infrastructure for a global distributed network of sensor networks requires secure authorization, authentication and access control facilities. There are a lot of PKI-based authentication and access control systems (e.g. Kerberos, OpenID, Shibboleth) that provide such basic services. We propose to apply a well-established, decentralized PKI-based authentication and authorization infrastructure to protect and simplify the inter-organizational access to the sensor network testbeds. Shibboleth[Shi] is an open source attribute-based access control system basing on state of the art cryptography and security protocols (e.g. X.509, PKCS, SAML, TLS/SSL). Single-Sign-On (SSO) is one of the key features of Shibboleth[Shi]. As illustrated in Figure 1, SSO massively improves the useability of remote resource access of several institution's resources. It facilitates the authorization and authentication process, and disburdens users from maintaining different access information (such as username, password) for every institution or even every resource they intend to access. Authorization of the requested resource access is based on the user attributes provided by the users' home organisation. Thus, all users from any institution within the Shibboleth federation can be authenticated to any Shibboleth-protected resource by using their home organisation accounts instead of getting a new user account locally. Currently, almost all Swiss universities and the universities of applied sciences are interconnected by the SWITCH Authentication and Authorization Infrastructure (AAI) [SWI04], which is the Shibboleth federation of the Swiss Higher Education System. The system is used by more than 175'000 students and researchers. Shibboleth will be used to combine all portals to sensor network testbeds affiliated with the WISEBED project, in order to create a unified system to grant access to the distributed sensor network testbeds - which is a key goal of the WISEBED project and a novelty in the research space of distributed wireless sensor network laboratories, as the integration of WSN testbeds into a compound network using Shibboleth [Shi] will be the first of its kind.

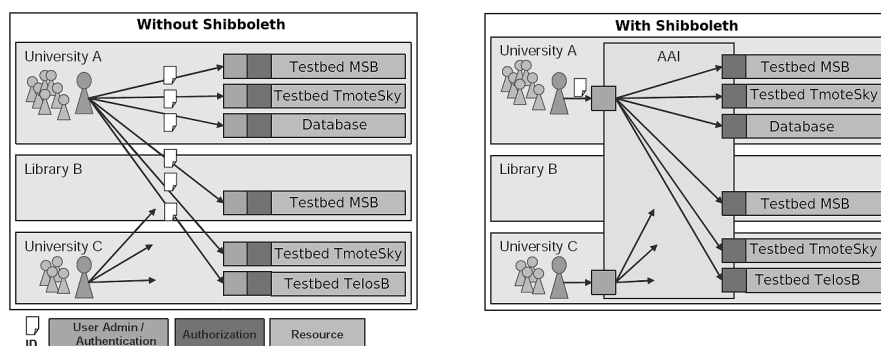


Figure 1: Inter-organizational testbed access with and without Shibboleth

In a first step, a Shibboleth federation has to be set up with all necessary components (Identity Provider (IdP), Where-Are-You-From server (WAYF), Discovery Service, etc). Each affiliated partner joins this federation and provides an own Identity Provider for its portal site. The Identity Provider hosts the site's user accounts, such that each affiliated partner is able to add own users and grant access to other user groups within the federation.

The application of Shibboleth constitutes a decentralized authorization and access control approach, and is therefore highly scalable to interconnect many organizations and numerous testbeds, and thus fits well for interconnecting distributed testbeds within WISEBED. Figure 2 illustrates Shibboleth protecting and controlling the remote access to the sensor network testbed portal servers. A login screen, as illustrated in Figure 3, is the entry point to the domain of the Shibboleth protected resources, where researchers choose their Home Organization in the list of federation members, and enter their credentials (username, password) once. We have recently been involved in projects where Shibboleth was applied for educational projects [BSW], [EU].

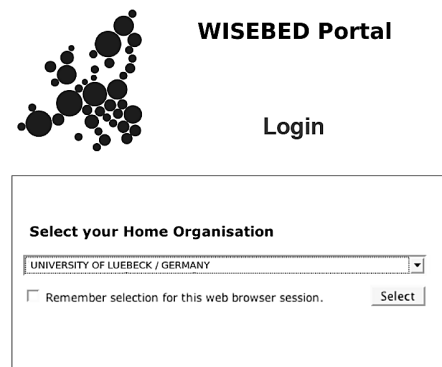
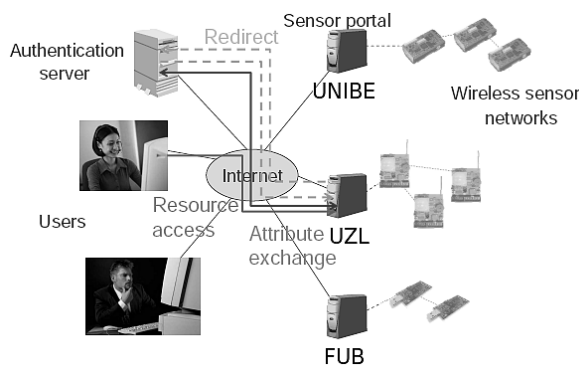


Figure 2: Shibboleth-protected WISEBED portals Figure 3: WISEBED portal login screen

3 Testbed Operation and Management System

3.1 Deployment of a Wireless Sensor Network Testbed

Design, deployment and maintenance of a wireless sensor network testbed is an inherently complex task. Integrating support for maintenance in the testbed planning process is of major importance and will definitely pay off in terms of personnel cost and efforts when it comes to testbed operation and maintenance. As nodes may crash or communication to nodes might become temporarily disrupted, a reliable tamper-proof backbone network should enable 7x24h backup remote access to every single node. Self-* features such as automatic reconfiguration and self-repair facilities are only possible when having wired backup links to each single sensor node. This avoids time-consuming costly on-site repairs and downtimes of the network.

3.2 Wireless Mesh Network Backbone

During the last few years, wireless mesh network (WMN) technologies have become very popular and mature. Several products are nowadays available off-the-shelf. Mesh nodes allow for

cost-efficient wired or wireless connectivity in local area networks. We suggest to co-deploy a mesh network operating as a communication backbone for all tasks concerning configuration, management, code distribution and recovery of the wireless sensor network nodes. Such a two-tiered hierarchical architecture consisting in mesh nodes and sensor nodes is currently being developed [WAB⁺08] to study the interconnection of heterogeneous sensor networks. A similar architecture has recently been designed and proposed in [BJGS08].

The wireless sensor nodes are connected to the mesh network backbone via either USB or RS232 links. The mesh network allows for fast and reliable remote access to all sensor nodes of the sensor testbed. In case of node failures, researchers shall be able to remotely trigger hard-resets by interrupting the mesh nodes' power supply to the sensor nodes. Researchers are therefore able to (re)configure and run sensor network experiments without having to be physically present. The mesh network is however intended to remain *behind the scenes* when it comes to algorithms and experiments to be run on the sensor network testbed.

Mesh nodes are connected among each other using IEEE 802.3 or IEEE 802.11 links. Wired links should be favored to avoid interferences with the sensor nodes. Depending on the sensor hardware and the respective radio transceivers, interferences with 802.11 WLAN devices are quite probable and could distort the results of algorithms running on the sensor nodes. As some nodes might however be placed at spots where no 802.3 Ethernet link is in physical reach, communication via 802.11a links should be envisaged, as transmissions in the 5GHz band do not interfere with most sensor radios and other surrounding wireless local area networks. Figure 4 illustrates our envisioned WSN testbed with the mesh network backbone. A Shibboleth-protected portal server connects the mesh backbone to the wired infrastructure of the university and is accessible from outside the university domain with a public IP address.

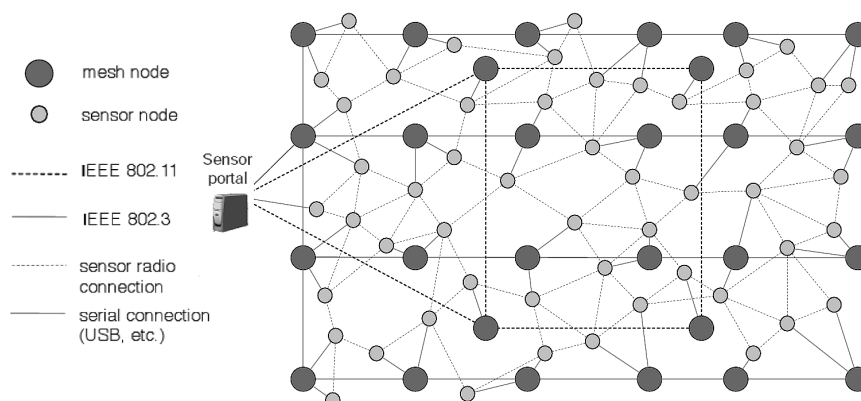
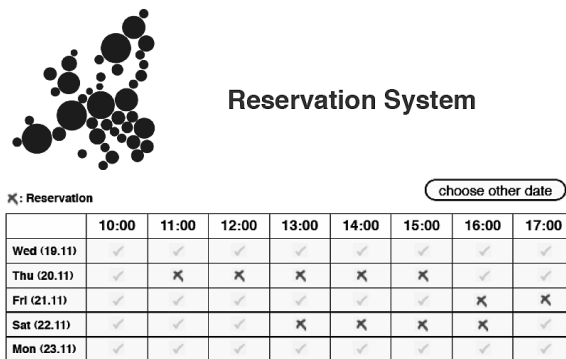


Figure 4: WSN testbed with mesh network backbone

3.3 Wireless Sensor Network Testbed Reservation System

In a heavily-used testbed, effective *scheduling* and *resource allocation* is important to allow a maximum number of users accessing a shared resource. A web-based reservation system facilitates the shared access of many researchers to the distributed wireless sensor network testbeds. After authentication and authorization using Shibboleth, researchers aiming to carry out

experiments on a WSN testbed can reserve time-slots during which they can access the network resources. The testbed reservation system displays an overview of the currently available un-allocated time-slots. The system allows reserving the time-slots and keeps track of the recent reservation activity of all actors on the testbed, in order to guarantee fair resource allocation. Researchers can immediately reserve the network resources and access the network in case there is nobody currently using it, or to schedule time-slots in the near future during which they will be granted access. Figure 5 illustrates a possible web-frontend where researchers can check the network's availability and schedule time for their experiments.

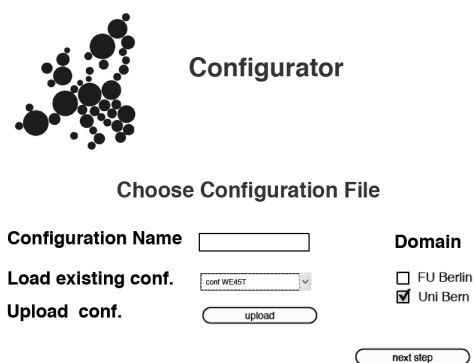


Reservation System

⌘: Reservation choose other date

	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00
Wed (19.11)	✓	✓	✓	✓	✓	✓	✓	✓
Thu (20.11)	✓	✗	✗	✗	✗	✗	✓	✓
Fri (21.11)	✓	✓	✓	✓	✓	✓	✗	✗
Sat (22.11)	✓	✓	✓	✗	✗	✗	✗	✓
Mon (23.11)	✓	✓	✓	✓	✓	✓	✓	✓

Figure 5: Testbed Reservation System



Configurator

Choose Configuration File

Configuration Name

Domain FU Berlin Uni Bern

Load existing conf.

Upload conf.

Figure 6: WSN Configurator

3.4 Wireless Sensor Network Testbed Configurator

After logging in and allocating a certain amount of time-slots of the testbed resources, researchers are guided to the WSN testbed Configurator. In a web-based interface, researchers obtain an overview about the configuration options the testbed offers. Researchers can select the nodes they intend to use and display their basic properties (e.g. id, location). The Configurator further lists all configurations that have been used during the last couple of testbed accesses, such that researchers can bypass time-consuming configuration steps if they intend to resume with the same configuration they had experimented with the day before. Depending on the sensor hardware that is used in the testbed, the Configurator allows uploading the most frequently used operating systems to the sensor nodes (e.g. TinyOS [tin] and Contiki [DGV04]). In a next step researchers can upload own applications and specify application-specific settings they intend to use for their experiments. The system pre-inspects the code by making sure that the code compiles for the requested platform and node types. After having completed all necessary configuration steps, the Configurator should check the settings for consistency, display the configuration settings in a summary screen and confirm the experiment setup.

4 Conclusions

In this paper we propose an infrastructure for secure remote authentication, management and operation of an interconnected network of wireless sensor network testbeds basing on the open source Shibboleth system. We describe our perspective of a web-based testbed management



system for remote wireless sensor network configuration and experimentation within a federation of distributed wireless sensor network laboratories.

Acknowledgements: This work has been supported by the 7th Framework Programme of the European Union under grant ICT-2008-224460 (WISEBED), the Swiss Science Foundation under grant 200020-113677/1, and the Hasler Foundation under grant ManCom 2060.

Bibliography

- [AER⁺06] A. Arora, E. Ertin, R. Ramnath, M. Nesterenko, W. Leal. Kansei: a testbed for sensing at scale. In *Intl. Conference On Information Processing In Sensor Networks (IPSN)*. 2006.
- [BBC⁺04] A. Bavier, M. Bowman, B. Chun, D. Culler, S. Karlin, S. Muir, L. Peterson, T. Roscoe, T. Spalink, M. Wawrzoniak. Operating System Support for Planetary-Scale Network Services. In *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*. 2004.
- [BJGS08] B. Blywis, F. Juraschek, M. Günes, J. Schiller. Design Concepts of a persistent Wireless Sensor Testbed. In *7. GI/ITG KuVS Fachgespräch Sensornetze*. 2008.
- [BSW] T. Braun, M.-A. Steinemann, A. Weyland. Realization of a Vision: Authentication and Authorization Infrastructure for the Swiss Higher Education Community. Educause November 2003.
- [DGV04] A. Dunkels, B. Gronvall, T. Voigt. Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors. In *29th Annual IEEE International Conference on Local Computer Networks (LCN)*. 2004.
- [EU] EU Lifelong Learning Programme. E-learning in Distributed Data Network Laboratory (EDINET). <http://www.svc-edinet.eu>, last visit Dec. 2008.
- [Shi] Shibboleth. An Internet2 middleware project. <http://shibboleth.internet2.edu>, last visit Dec. 2008.
- [SWI04] SWITCH. The Swiss Education and Research Network - Authentication and Authorization Infrastructure: System and Interface Specification. 2004.
- [tin] TinyOS. <http://webs.cs.berkeley.edu/tos/>, last visit Dec. 2008.
- [Tut] Tutornet. A tiered wireless sensor network testbed. <http://enl.usc.edu/projects/tutornet>, last visit Dec. 2008.
- [WAB⁺08] G. Wagenknecht, M. Anwander, T. Braun, T. Staub, J. Matheka, S. Morgenthaler. MARWIS: A Management Architecture for Heterogeneous Wireless Sensor Networks. 6th Wired/Wireless Internet Communications: 6th International Conference (WWIC), 2008.
- [Wir] Wireless Sensor Networks Testbed (WISEBED). Seventh Framework Programme FP7. <http://www.wisebed.eu>, last visit Dec. 2008.
- [WSW05] G. Werner-Allen, P. Swieskowski, M. Welsh. MoteLab: A Wireless Sensor Network Testbed. In *ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN-SPOTS)*. 2005.