WSNLab – a Security Testbed and Security Architecture for WSNs

Nils Aschenbruck°•, Jan Bauer°, Jakob Bieling°, Alexander Bothe°, Matthias Schwamborn°
° University of Bonn - Institute of Computer Science 4, Friedrich-Ebert-Allee 144, 53113 Bonn, Germany
• Fraunhofer FKIE, Neuenahrer Str. 20, 53343 Wachtberg, Germany
{aschenbruck, bauer, bieling, bothea, schwamborn}@cs.uni-bonn.de

I. Motivation

A Wireless Sensor Network (WSN) consists of small, resource-constrained computing devices (so-called motes) that perform physical measurements (e.g., temperature, vibration) in a distributed manner. The motes form a self-adaptive multi-hop network to transport the measured data to a sink. The data may be pre-processed and fused in the network. Furthermore, WSNs often provide capabilities using a reverse channel for sensor control and management as well as flashing of motes and Over-The-Air Programming (OTAP). WSNs are deployed in a steadily growing plethora of application areas. Especially their deployment in the industrial, military, public safety, and medical domains renders security in these networks an issue of high relevance.

There is a need for a real-world security testbed for the evaluation of WSN security measures. Given such a lab, a security architecture for WSN can be developed, implemented, and evaluated. The rest of this abstract is structured as follows: The testbed is described in Section II. Next, we present a threat analysis and security architecture for WSNs (Section III). In the demo, we will show our WSN testbed as well as the Intrusion Detection System (IDS).

II. The Security Testbed

For the testbed, different WSN hardware and software platforms are considered to reflect realism through heterogeneity. In its current setup, the testbed consists of three Operating Systems (OSs) (Contiki [5], iSense [4], and TinyOS [10]) running on three hardware platforms (TelosB [13], MicaZ [12], and iSense-CM10C [11]). For the WSNLab testbed, we realized three sub-networks with different OSs. The different sub-networks are separated physically using different radio channels, as the standard Media Access Control (MAC) protocols of the different OSs are not interoperable. A solution for the future may be the use of IEEE 802.15.4 MAC protocol implementations. However, to the best of our knowledge, there is only an implementation for TinyOS available [9] up to now.

The deployed application consists of a simple distributed sensor data collection process. Motes sense and transmit the sensor data to the sink. As self-adaptive WSN routing protocols, the Collection Tree Protocol (CTP) [8] and the IPv6 Routing Protocol for Low power and Lossy Networks (RPL) [16] are used to deliver sensor data via multiple hops. Thus, the sensor data can be delivered even though the sink is not in direct communication range.

To realize multi-hop paths in a reliable and reproducible way, the testbed supports topology management using a link control system based on the concept of virtual links (cf. [3]). Even complex topologies can be defined by manipulating the delivery of messages. On each mote, there is a module that checks whether packets received over the air are supposed to reach the receiving mote based on the defined topology. These topologies can even be changed during an experiment. The motes become virtually mobile. By doing so, mobile sensor networks can be evaluated in the testbed as well. Figure 1 visualizes the integration of mobility into the testbed. Arbitrary scenarios using different mobility models [2] can be used through the integration of BonnMotion [1]. BonnMotion supports WiseML [14], a scenario and experiment specification language for WSNs that is based on GraphML, an XML dialect. The goal of WiseML is to specify inputs and outputs and enabling the reproduction of experiments. The WiseML files are used as input for the link control system. Overall, the testbed can be used to evaluate WSN algorithms and protocols in heterogeneous, complex, static and mobile scenarios.

For evaluation purposes, we added a Jackdaw IEEE 802.15.4 Sniffer [15] (running Contiki) to the testbed. This device allows us to capture all packets of a wireless channel and analyze them using packet analyzer tools like Wireshark [17]. Moreover, we added a GNU Radio [7] USRP-Board [6] to the testbed. This special hardware allows us to run various types of Jamming attacks.

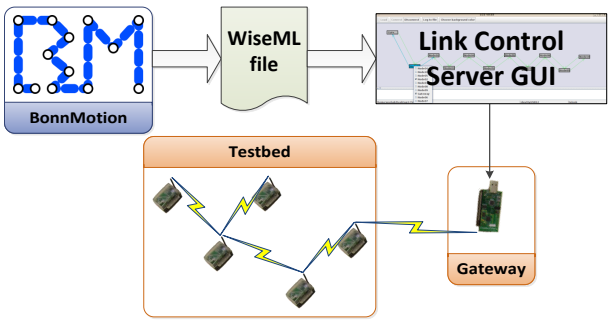

Fig. 1. Integrating mobility in the WSNLab testbed.

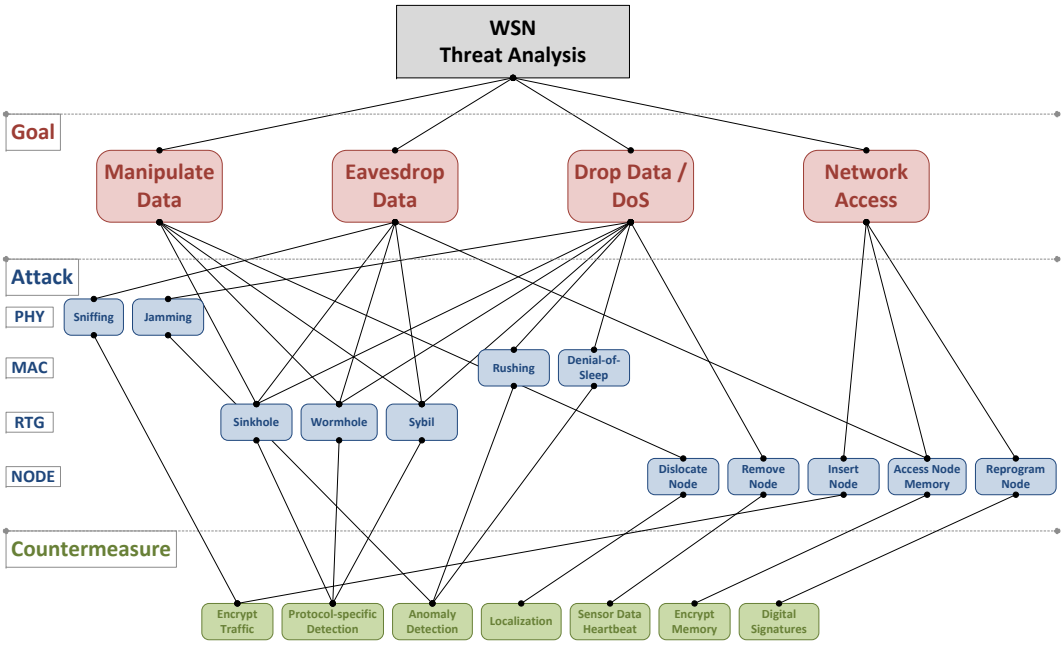

Fig. 2. Threat analysis and countermeasures for WSNs.

III. The Security Architecture

An attacker can achieve his objective(s) through different kinds of attacks. These can be categorized based on the targeted layer. Figure 2 shows a threat analysis as well as countermeasures for WSNs. The threat analysis is first divided into the goals of the attacker.

The specific properties of WSNs lead to special attacks as well as new challenges for countermeasure development: The resource scarcity of the nodes in terms of computing power, memory, energy, and bandwidth requires countermeasures to be light-weight but also effective at the same time. We have implemented a security architecture based on the countermeasures mentioned (cf. Figure 2). Preventive measures such as traffic encryption and digital signatures were implemented on the motes. The detection measures were integrated in an IDS. Figure 3 shows the architecture of the IDS. The IDS server receives status and alarm messages generated by an IDS module on the motes. The server analyzes these messages using different anomaly detection algorithms, e.g., based on statistical or aging functions. In the current version, the following attacks are detected by the IDS:

- *Remove Node* triggering the heartbeat and movement modules,
- *Dislocate Node* triggering the movement module,
- *Jamming* triggering the Carrier-Sense-Time module,
- *Reprogram Node* triggering the OTAP module.

Based on the analysis of the server, alarm messages are generated and visualized using an IDS graphical user interface. The design of the IDS is modular. Thus, further modules can be easily integrated. However, the resource scarcity of the nodes limits the number of modules that can be used simultaneously.

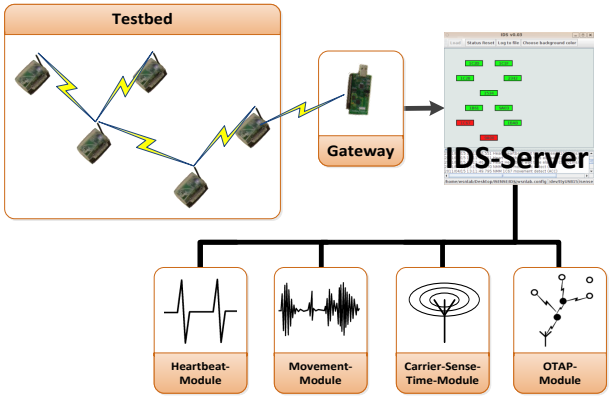

Fig. 3. WSNLab IDS architecture.

Acknowledgments

This work was supported in part by the German Federal Office for Information Security (BSI). Furthermore, this work was supported in part by CONET, the Cooperating Objects Network of Excellence, funded by the European Commission under FP7 with contract number FP7-2007-2-224053. The authors would like to thank the WSNLab and CONET project teams for feedback, sustainable discussion, and work.

REFERENCES

[1] N. Aschenbruck, R. Ernst, E. Gerhards-Padilla, and M. Schwamborn, "BonnMotion - a Mobility Scenario Generation and Analysis Tool," in *Proc. of the 3rd Int. ICST Conference on Simulation Tools and Techniques (SIMUTools '10)*, Torremolinos, Spain, 2010, pp. 1–10.

[2] N. Aschenbruck, A. Munjal, and T. Camp, "Trace-based Mobility Modeling for Multi-hop Wireless Networks," *Elsevier Computer Communications*, vol. 34, no. 6, pp. 704–714, 2011.

[3] T. Baumgartner, I. Chatzigiannakis, M. Danckwardt, C. Koninis, A. Kröller, G. Mylonas, D. Pfisterer, and B. Porter, "Virtualising Testbeds to Support Large-Scale Reconfigurable Experimental Facilities," in *Proc. of the 7th European Conference on Wireless Sensor Networks (EWSN '10)*, Coimbra, Portugal, 2010, pp. 210–223.

[4] C. Buschmann and D. Pfisterer, "iSense: A Modular Hardware and Software Platform for Wireless Sensor Networks," 6. Fachgespräch "Drahtlose Sensornetze" der GI/ITG-Fachgruppe "Kommunikation und Verteilte Systeme", Tech. Rep., 2007. [Online]. Available: http://ds.informatik.rwth-aachen.de/events/fgsn07

[5] A. Dunkels, B. Grönvall, and T. Voigt, "Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors," in *Proc. of the 29th Annual Conference on Local Computer Networks (LCN '04)*, Tampa, Florida, USA, 2004, pp. 455–462.

[6] Ettus Research LLC, "Universal Software Radio Peripheral – Motherboard Datasheet," 2011. [Online]. Available: http://www.ettus.com/downloads/ettus_ds_usrp_v7.pdf

[7] Free Software Foundation, "GNU Radio," 2011. [Online]. Available: http://gnuradio.org/redmine/wiki/gnuradio

[8] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection Tree Protocol," in *Proc. of the 7th Conference on Embedded Networked Sensor Systems (SenSys '09)*, Berkeley, California, USA, 2009, pp. 1–14.

[9] J.-H. Hauer, R. Daidone, R. Severino, J. Büsch, M. Tiloca, and S. Tennina, "Poster Abstract: An Open-Source IEEE 802.15.4 MAC Implementation for TinyOS 2.1," in *Proc. of the 8th European Conference on Wireless Sensor Networks (EWSN '11)*, Bonn, Germany, 2011.

[10] J. L. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. S. J. Pister, "System Architecture Directions for Networked Sensors," in *Proc. of the 9th Int. Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '00)*, Cambridge, Massachusetts, USA, 2000, pp. 93–104.

[11] iSense, "Core Module CM10C, CM10S Preliminary Data Sheet," 2011. [Online]. Available: http://www.coalesenses.com/download/CM10X_DS_1v1.pdf

[12] MEMSIC, "MicaZ datasheet," 2011. [Online]. Available: http://www.memsic.com/support/documentation/wireless-sensor-networks/category/7-datasheets.html?download=148

[13] ——, "TelosB datasheet," 2011. [Online]. Available: http://www.memsic.com/support/documentation/wireless-sensor-networks/category/7-datasheets.html?download=152

[14] Seventh Framework Programme FP7 – Information and Communication Technologies (ICT), "WiseML schema," 2011. [Online]. Available: http://dutigw.st.ewi.tudelft.nl/wiseml/wiseml_schema.pdf

[15] Swedish Institute of Computer Science (SICS), "RZRAVEN USB Stick (Jackdaw)," 2011. [Online]. Available: http://www.sics.se/~adam/contiki/docs-uipv6/a01108.html

[16] T. Winter and P. Thubert, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," Internet Engineering Task Force, Draft, 2011. [Online]. Available: http://tools.ietf.org/html/draft-ietf-roll-rpl-19

[17] Wireshark Foundation, "Wireshark – The world's foremost network protocol analyzer," 2011. [Online]. Available: http://www.wireshark.org