ESAWN-NR: Authentic Aggregation and Non-Repudiation in Wireless Sensor Networks

Joachim Wilke Erik-Oliver Blaß Martina Zitterbart
Institute of Telematics
University of Karlsruhe, Germany
Email: {wilke,blass,zit}@tm.uka.de

This demonstration shows ESAWN-NR in action, a protocol for authentic, yet efficient data aggregation in presence of malicious, compromised sensor nodes. ESAWN-NR does not only achieve authenticity of data aggregates, but also allows to prove *forged* aggregates coming from specific nodes. This allows easy exclusion of such nodes from the network.

ESAWN-NR Protocol

ESAWN-NR is based on ESAWN ("**E**xtended **S**ecure **A**ggregation for **W**ireless Sensor **N**etwork"), published in [1]. ESAWN-NR extends ESAWN by providing these properties:

(1) Forged data is not only detected, but also automatically *corrected* by non-compromised, legitimate nodes.

(2) A compromised node cannot *repudiate* its forgery at a later time.

ESAWN-NR assigns *witness nodes* to every aggregation node to reproduce aggregates. This results in a set U of data belonging to the same aggregate. Therewith, ESAWN-NR utilizes aggregate-comparison to *detect* forged data within U and, by *majority-vote*, computes a corrected aggregate to achieve the aforementioned security property *(1)*. To achieve property *(2)*, data is not directly sent to the sink, but firstly routed towards other witness nodes for *monitoring* and temporary *logging* of all data sent. As a result, legitimate nodes are enabled to not only detect and correct forged data, but also identify and prove the existence of compromised nodes to other legitimate nodes.

Demo Details

ESAWN-NR is implemented within TinyOS. The demonstration is shown using MicaZ motes. One node is connected to a notebook. Together they represent the "sink" of the network, providing network-access to the user. The other nodes act as aggregating or measuring nodes. This is configured by the demonstration application running on the notebook. It also allows to configure the network structure and topology, i.e., the routing within the network. Finally, you can choose, which nodes are *compromised*, i.e., behave maliciously and try to forge data. A wireless packet monitor on the notebook shows all traffic sent within the sensor-network and helps understanding ESAWN-NR's protocol-execution and activity. Fig. 1 shows the demonstration setup.

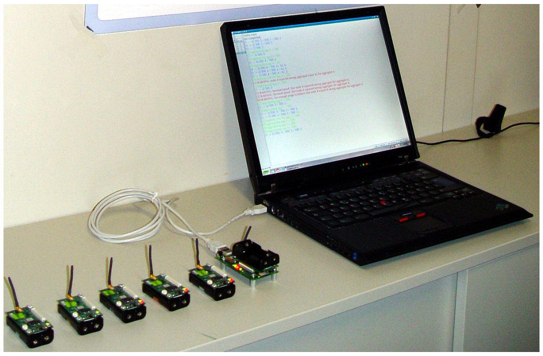

Fig. 1. Demonstration setup

For simplicity, prior to execution of ESAWN-NR, a sensor node receives its configuration, e.g., its routing neighbors and the cryptographic keys required for communication, from the sink. After all nodes are configured, the sink floods a "request-for-data query" into the network and ESAWN-NR is started. Three LEDs on each sensor show its current status. *Green* indicates an idle but already initialized node: the node is ready for execution of ESAWN-NR, having all necessary keys and network configuration knowledge. *Yellow* indicates activity, e.g., an aggregation in process. *Red* indicates the detection of a compromised node.

Every message sent in the network and all node activity is logged by the packet monitor and visualized in the demonstration application to help understanding the protocol's activity. Three classes of messages are shown in the application: *1.)* messages representing ESAWN-NR's data-packets, *2.)* messages describing internal node-activities, such as the computation of an aggregate or a "majority-vote" used by ESAWN-NR, *3.)* messages showing activities necessary because of the detection and elimination of a compromised node. This includes detection of forged values during a majority-vote and the notification of the existence of specific compromised nodes sent to other legitimate nodes. To simplify understanding the protocol execution, ESAWN-NR's operations are slowed down, e.g., the calculation of an aggregate takes about 4 seconds. By varying the network-structure, ESAWN-NR's protocol parameters, or by compromising multiple nodes, ESAWN-NR's behavior in different situations can be explored and analyzed.

ESAWN-NR has already been theoretically analyzed and evaluated by simulations. It has been shown to be more energy-efficient than authentic, but non-aggregating communication. This demonstration on MicaZ motes shows the feasibility of ESAWN-NR on resource-limited hardware.

References

[1] E.-O. Blaß, J. Wilke, and M. Zitterbart, "A security–energy trade-off for authentic aggregation in sensor networks," in *IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Washington D.C., USA, Sep 2006, pp. 135–137.