AUTHENTIC QUERY DISSEMINATION AND DATA AGGREGATION IN WSN

Joachim Wilke[1], *Zinaida Benenson*[2], *Martina Zitterbart*[1], *Felix C. Freiling*[2]
[1]Institute of Telematics, Universität Karlsruhe (TH), Germany
[2]Department of Computer Science, University of Mannheim, Germany

In a public wireless sensor network (WSN), the presence of *adversaries* that can completely take over some sensor nodes must be taken into account. The adversary may try to use the compromised nodes to inject his own *queries* or to influence results of legitimate queries, when they are propagated to the network's sink during *data concast*. Because of the commonly used paradigm of *in-network processing*, a compromised node can manipulate all passing data easily. Hence, the *authenticity* of both, query and result, must be verified. However, providing authenticity needs additional effort, which increases energy-consumption. We present AQF+ESAWN, the (to our knowledge) first attempt to provide an integrated solution for authentic query processing *and* data concast in WSNs in an energy-efficient, configurable way. Before describing the benefits of this demonstration, we shortly sketch the two protocols AQF and ESAWN and the energy-authenticity trade-off provided.

Query processing

In a WSN, only *legitimate* entities should be able to send queries into the network. Queries from an adversary should be detected and dropped. To solve this problem, we propose the **A**uthenticated **Q**uery **F**looding protocol [1], which is a variant of broadcast authentication. It assigns an *authentificator* of size m to each query. Based on the authentificator and a specific key pre-distribution D, each node is able to verify the authenticity of a query with a certain probability $\mathcal{P}_Q(m, D)$. AQF is the first *gracefully degrading* broadcast authentication protocol that enables to trade-off consumed energy against detection probability: the higher m, the larger $\mathcal{P}_Q$. On the other hand, the higher m, the larger the query and the larger the energy consumed.

Data concast

Using in-network-processing like *data aggregation* in WSNs is essential to reduce communication volume and thus achieve energy-efficient data delivery. However, nodes compromised by an adversary can modify aggregates in arbitrary ways. **E**xtended **S**ecure **A**ggregation for **W**ireless sensor **N**etworks [2], [3] is a concast protocol utilizing data aggregation for energy-efficiency while providing *probabilistic authenticity* of the received results. ESAWN assigns k *witness nodes* to every aggregation node to recompute aggregates. If there is a difference between the values computed by the aggregation nodes and the values computed by the witnesses, an *alarm* is sent to the sink and the aggregation is stopped. The higher k, the higher the level of authenticity provided, but also the higher the protocol's energy consumption. Assuming a certain upper bound β of compromised nodes, ESAWN gives a probabilistic guarantee $\mathcal{P}_C(k, \beta)$ for an aggregate being authentic.

AQF+ESAWN

Protocol integregation allows to identify commonly used parts to share, i.e., using the same efficient symmetric cryptographic primitives. Furthermore, we tightly couple both protocols: During query dissemination (by flooding), an aggregation structure to be used by ESAWN for result concast is set up. Receiving an AQF-query initiates sensor reading and data concast by ESAWN. Most important, adjusting the parameters m (for AQF) and k (for ESAWN) allows to trade-off energy and authenticity for both query dissemination and data concast in a coordinated manner.

Demo details

AQF+ESAWN is implemented within TinyOS. The demo setup uses several MicaZ nodes and a notebook. The latter represents the base station providing network access to the user and running the demo frontend. The frontend, written in Java, visualizes the network configuration, including communication and node states, and a chronological event list. For demo purposes, we limited the transmission range of our devices to less than 15 cm. This way, we are able to emulate a multi-hop network on a single table.

The audience can experiment with different protocol and network settings in order to examine the trade-off between security and energy consumption of the protocols. They can set security parameters of the protocol, change network configuration by moving the nodes around and compromise arbitrary nodes using an integrated "malicious mode" that can be activated in the configuration dialog of the demo-frontend.

The purpose of this demo is not only to prove the feasibility of AQF+ESAWN on resource-limited hardware, but to show the concept of probabilistic, gracefully degrading security as a promising direction for energy efficient security for WSNs: In presence of node compromise attacks to a certain upper bound, our framework guarantees that query and result are authentic with a pre-defined probability. First results prove AQF+ESAWN to be significantly more flexible and energy-efficient than conventional authentication schemes.

References

[1] Z. Benenson, F. C. Freiling, E. Hammerschmidt, S. Lucks, and L. Pimenidis, "Authenticated Query Flooding in Sensor Networks," in *Proceedings of the IFIP TC-11 SEC 2006*, 2006, pp. 38–49.

[2] E.-O. Blaß, J. Wilke, and M. Zitterbart, "Relaxed Authenticity for Data Aggregation in Wireless Sensor Networks." Istanbul, Turkey: SecureComm, Sep. 2008, ISBN 978-1-60558-241-2.

[3] J. Wilke, E.-O. Blaß, and M. Zitterbart, "ESAWN-NR: Authentic Aggregation and Non-Repudiation in Wireless Sensor Networks." Kanazawa, Japan: INSS, Jun. 2008, p. 254, ISBN 978-4-907764-31-9.