

Security Solutions for Wireless Sensor Networks

Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA

Abstract

This paper describes security solutions for collecting and processing data in Wireless Sensor Networks (WSNs). Adequate security capabilities for medium and large scale WSNs are a hard but necessary goal to achieve to prepare these networks for the market. The paper includes an overview on security and reliability challenges for WSNs and introduces a toolbox concept to support such a framework.

Keywords

Wireless Sensor Networks (WSN), security, volatile environments

1. Introduction

Wireless Sensor Networks (WSNs) use tiny, inexpensive sensor nodes with several distinguishing characteristics: they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific monitoring and sensing functions. Several such wireless sensors in a region self-organize and form a WSN. Information based on sensed data can be used in agriculture and livestock, assisted driving or even in providing security at home or in public places. A key requirement from both the technological and commercial point of view is to provide adequate security capabilities. Fulfilling privacy and security requirements in an appropriate architecture for WSNs offering pervasive services is essential for user acceptance. Five key features need to be considered when developing WSN solutions: scalability, security, reliability, self-healing and robustness. The required strength of each of these features depends on the application in question. The paper is structured as follows: In Section 2, we look at the background of sensor networks and their distinguishing characteristics. Section 3 follows up by identifying the research areas that need to be covered, while Section 4 describes the solutions we have developed so far in the context of the EU collaborative project UbiSec&Sens. Section 5 concludes.

2. Background on Sensor Networks

2.1 Technology

WSNs form a particular class of ad hoc networks that operate

with little or no infrastructure. WSNs are gaining momentum as they have great potential for both research and commercial applications. The sensor network nodes themselves are ideally low-priced, very small devices. They typically consist of a collection of application specific sensors, a wireless transceiver, a simple general purpose processor, possibly assisted by limited amount of special-purpose hardware, and an energy unit that may be a battery or a mechanism to obtain energy from the environment. We cannot assume that sensor nodes will be tamper-resistant, although we will consider the availability of such tamper-resistant nodes for future applications. Sensor nodes are distributed over a potentially vast geographical area to form a static, multi-hop, self-organizing network. However, also mobile WSNs and mobility within WSN are conceivable.

2.2 Threat Models and Their Relevance in WSNs

Typical functions in a WSN include sensing and collecting data, processing and transmitting sensed data, possibly storing data for some time, and providing processed data as information e.g. to a so called sink node. A particular kind of processing that is essential, as will be explained later, is aggregation of data in the sensor nodes. Securing such functions turns out to be very challenging. The Dolev-Yao¹⁾ threat model often used to formally analyze crypto-protocols in communication networks has its limitations in the context of WSNs and for ubiquitous computing.

The Dolev-Yao threat model assumes that the two communicating parties, say A(lice) and B(ob), communicate over an insecure channel. If an intruder gains control over the communication network, she/he can overhear messages between the partners, intercept them and prevent their delivery to the intended recipient. But this threat model also assumes that the

end-points, Alice and Bob, are not themselves subject to attack. A WSN adapted threat model should reflect that the channel is assumed to be insecure and the end-points cannot in general be trusted. An attacker may physically pick up sensor nodes and extract sensitive information.

2.3 Probabilistic Security

To limit damage as described in the previous sub-section, we could take two distinct approaches:

- 1) Using “tamper-resistant units”: Each sensor node is equipped with a tamper-resistant component for the storage of sensitive e.g. key data, thus limiting the damage following the capture of nodes.
- 2) Aiming at “probabilistic security”: In this setting, we do not assume that sensor nodes are tamper-resistant, but rather limit what an attacker gains after reading data from captured sensor nodes.

Because of the high cost, the first option will be restricted to application domains that are critical enough to be more expensive or requiring few sensors. If devices cannot be made tamper-resistant, we will aim at probabilistic security. In this approach, the term “limited gain” expresses that the attacker receives only a “well-defined” subset of knowledge from the WSN.

2.4 Design Space of Security Solutions

Nodes that compose a WSN are typically small and have very limited communication, computation, storage and power capabilities. The Berkeley Motes²⁾ use an 8-bit 4MHz Microcontroller (MCU) with 4KB of memory and a radio transceiver with a maximum of 10kbps data rate. To keep costs low, most sensors are not tamper-resistant, which impacts security. Limited computing and storage capabilities make modular arithmetic with large numbers difficult and thus asymmetric (public key) cryptography unsuitable. In particular, the classical Diffie-Hellman (DH) key exchange protocol is excluded. Even low exponent variations of the Rivest, Shamir and Adleman (RSA) scheme are prohibitively expensive for a sensor. Extremely low-cost mechanisms that do not require processor-intensive operations are needed. Also, sending a bit is roughly 102 times more expensive than executing a processor instruction. The data transmitted can be reduced by using data aggregation, i.e. combining data (values) at the nodes.

3. Key Research Areas

We identified the three key research areas “Security&Reli-

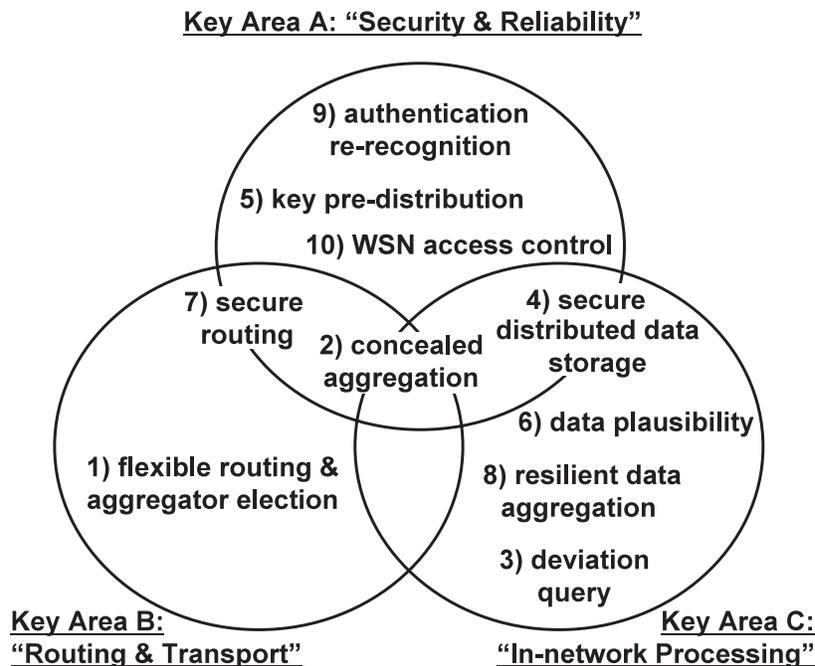


Fig. 1 WSN key research areas.

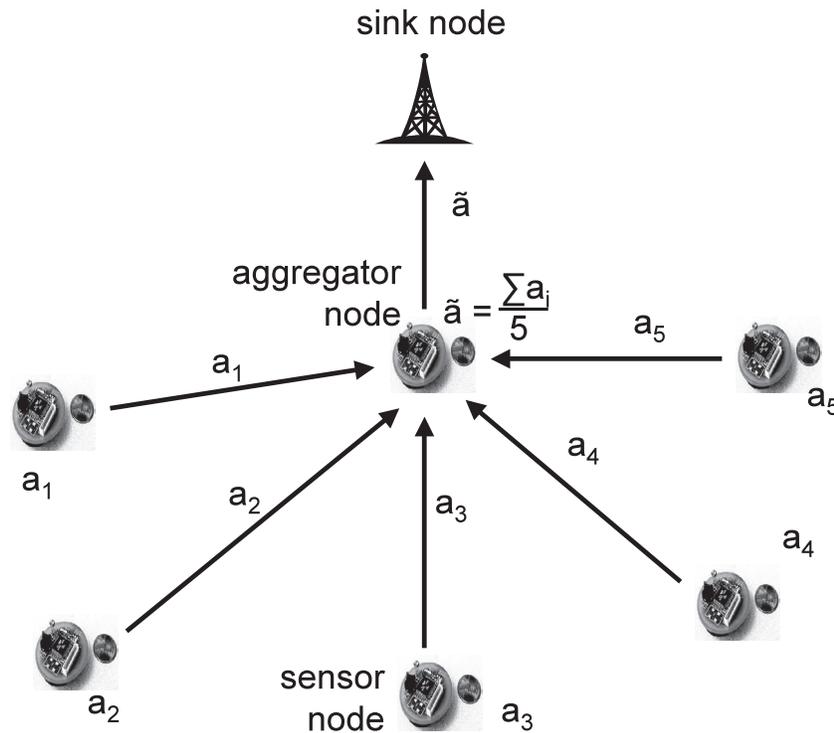


Fig. 2 Reverse multicast traffic with in-network processing.

ability”, “Routing&Transport” and “In-network Processing” for developing secure and reliable WSNs (Fig. 1). Solutions for the first take into account the extended Dolev-Yao model, aiming at probabilistic security.

The top-ten related research topics from the above research areas are:

1) Flexible routing and aggregator election: The configured WSN must be flexible enough to cope with gradually or abruptly disappearing nodes. The overall scheme must support routing and multiple levels of in-network processing. Fig. 2 illustrates the pre-dominant traffic pattern for a WSN with only one level of aggregator nodes containing a single aggregator node. To exemplify, the aggregation function performed at the aggregator node is “average.” In large WSNs multiple aggregator nodes and multiple levels of aggregator nodes are used. Re-election of aggregator nodes can help balance the energy-consumption in the WSN.

2) Concealed data aggregation: It is a concern within WSNs to both reduce the energy consumption at the sensor nodes and the effect of physical attacks on the nodes. Enhanced mechanisms for end-to-end encryption from the sensors to the sink, also termed reverse multicast traffic, addresses this

concern. Concealed Data Aggregation provides a good balance between energy-efficiency and security while still allowing data to be processed at the sensor nodes. The aggregator node in Fig. 2 is the one that should be able to aggregate encrypted data.

3) Data aggregation based on deviation query and multiple monitoring sensors: For a condensed representation and transmission of the monitored data, it is useful to transmit more than one type of values, e.g. temperature and humidity, within one message. It may even help to transmit only the deviation values from a pre-defined basis, since this helps to reduce the amount of data to be transmitted.

4) Secure distributed data storage: In some applications, monitored data must be stored in a distributed way. Whenever it is undesirable or impossible to transmit volatile, regional information to an authorized querying party in real-time, the WSN itself needs to store the monitored data. Since the WSN environment is volatile with nodes that disappear over time, security must be combined with replication, taking space- and energy-efficient storage into consideration.

5) Enhanced key pre-distribution: It is not possible for the manufacturer to configure all the sensitive information, such

as keys, before the WSN is rolled-out. Some sensitive information can only be determined and stored with knowledge of the final position of the nodes within the network topology. Also, the traffic pattern, i.e. how data is expected to flow in the network, is another parameter to consider when distributing keys.

6) Data plausibility: For some applications, we must check the plausibility of the received and aggregated data at the sink node. Since a plausibility check always requires some redundant information, we need a trade-off between accuracy and efficiency. A plausibility check also needs to consider the semantics of the specific WSN application. It is necessary to investigate dependencies and trade-offs for an appropriately accurate and efficient plausibility check at some well-defined points of the WSN for the respective solutions.

7) Provably secure routing: Routing is one of the most basic networking functions in multi-hop sensor networks. The presence of malicious nodes must be considered and precautions taken. Routing has two main functions: finding routes to the sink nodes, and forwarding data packets via these routes. Security approaches for routing protocols have mainly been analyzed by informal means only. What is needed is a mathematical framework in which security can be precisely defined.

8) Resilient data aggregation: This item addresses how to make data aggregation at nodes robust and resilient in the presence of an adversary that can modify the input data. A solution should address data aggregation both at the sink node and at sensor nodes. Any solution must consider a minor rate of false negatives and abide with it.

9) Pairwise/groupwise authentication: In the most general case, nodes need to build up a well-defined security association without any pre-established secret or common security infrastructure. In this case, pairs of entities will establish pair-wise relationships. It is also conceivable that groups of entities are able to establish new relationships. Any such authentication or re-recognition scheme must also take energy-consumption and storage requirements into consideration.

10) WSN access control: it is essential to provide an access control for end-users of WSN applications that ensures access to the monitored data for authorized parties only, supports user-friendly data queries and is DoS resilient to save the sensors' battery capacity.

4. The UbiSec&Sens Project

The European Specific Target Research Project (STReP)

UbiSec&Sens - "Ubiquitous Security and Sensing in the European Homeland" (Jan. 2006 - Dec. 2008) aims at providing a security architecture for the research areas identified in Section 3 and a set of WSN applications and scenarios (agriculture, road and homeland security). The project is working towards a toolbox of security-aware components, depicted in **Fig. 3**, which will be easy to configure by manufacturers and service developers to create security support for upcoming wireless sensor network applications. The project is following the probabilistic security paradigm for the following research areas:

4.1 Authentication and Re-Recognition

One of the major threats in WSNs is the presence of an adversary that injects forged data in the network or pretends to be an aggregator. Current mechanisms for authentication are based on complex computations, such as public key cryptography, which are not applicable in WSNs. In most scenarios, an authority issuing shared secrets is not available, as the sensors tend to communicate in a decentralized manner. With the Zero Common Knowledge (ZCK) protocol² we provide an authentication protocol that establishes well-defined pair-wise security associations between entities in the absence of a common security infrastructure or pre-shared secrets. We show that with two keyed hash-chains per communication pair, one can establish a certain level of trust within the system; ZCK ensures the re-recognition of a communication partner.

4.2 Concealed Data Aggregation

The Concealed Data Aggregation (CDA)³ approach proposes to use symmetric additively homomorphic encryption transformations for end-to-end encryption of sensed data for reverse multicast traffic between the monitoring sensor nodes and the sink node. CDA enables intermediate aggregator nodes to aggregate ciphers without the cost of decrypting and re-encrypting these messages. These aggregator nodes are not required to store sensitive keys. Aggregation supported by CDA is based on homomorphic encryption transformations, and cover averaging, movement detection and variance functions. In Reference 5), we show how the order preserving encryption scheme is used to compare encrypted data to extend the set of aggregation functions to include the minimum and maximum of the sensed values. We have implemented this scheme on sensor nodes.

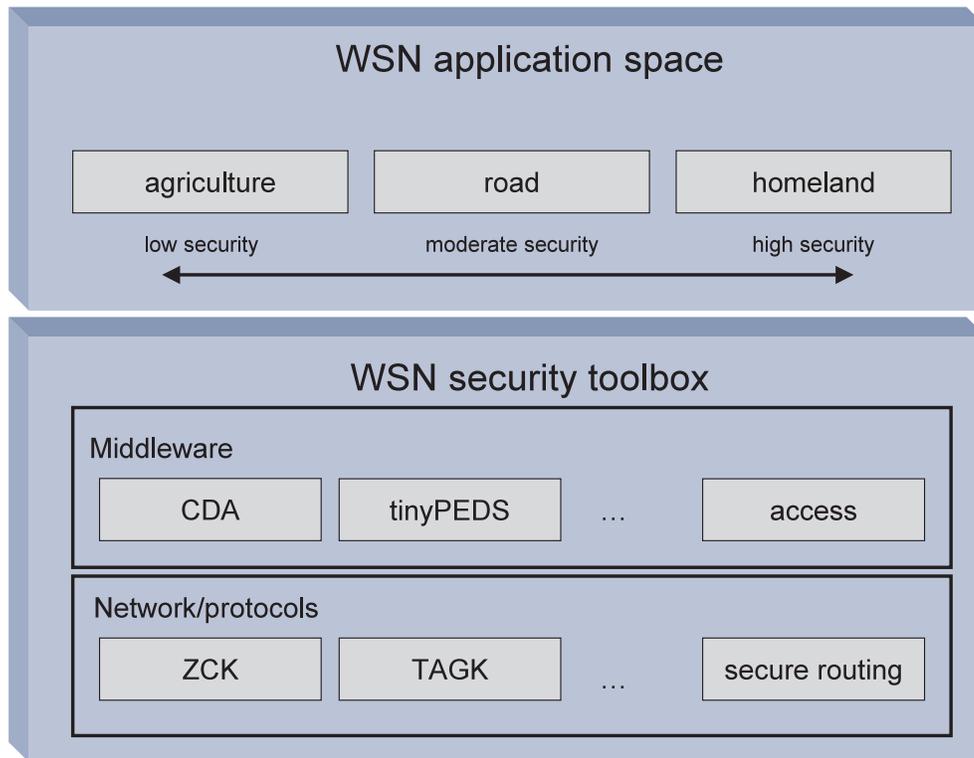


Fig. 3 The UbiSec&Sens toolbox concept.

4.3 Key Pre-Distribution

The issue of key pre-distribution and its adaptation to the major traffic pattern “reverse multicast traffic” is addressed in Reference 3) by introducing Topology Aware Group Keying (TAGK). During the WSN’s roll-out and its initial bootstrapping phase, all available nodes discover, in a fully self-organized and topology-aware manner, their neighbors and specific roles. TAGK establishes mutually disjoint regions with randomly chosen group keys per epoch and region for reverse multicast traffic. It provides probabilistic security and is essential to be able to use CDA. We have simulated very large WSNs, which confirm the feasibility and scalability of the approach. We have also implemented this scheme.

4.4 Secure Distributed Data Storage

We are currently exploring the collaborative storage of encrypted data in WSNs, similar to a distributed database. In sensor network applications with asynchronous character and only temporary connection to the sink node, nodes need to aggre-

gate and store the monitored data of their surroundings over a certain period to be able to respond to query requests at a later time. An adversary should not be able to obtain any sensitive data stored on the nodes. The Persistent Encrypted Data Storage (tinyPEDS) approach⁶⁾ proposes an architecture for reliable and secure in-network storage of the monitored data by applying (realistic) asymmetric additively homomorphic encryption transformation⁷⁾ with aggregation capabilities for long term data storage. Together with the query process that retrieves the stored values, tinyPEDS also provides a recovery mechanism for values affected by a disaster scenario, where a considerable part of the network abruptly disappears. tinyPEDS has been subjected to validation by simulation and we are now in the process of implementing it for the sensor platform.

UbiSec&Sens solutions will be prototyped and validated in the representative wireless sensor application scenarios of agriculture and road services. We also refer to <http://www.ist-ubisecsens.org>.

5. Conclusion

We described security and reliability challenges for WSNs. Within the STReP UbiSec&Sens*, we analyze three complementary WSN applications with the goal of developing a modular toolbox to support an integrated security and reliability architecture for medium and large-scale WSNs.

*The work presented in this paper was supported in part by the European Commission within the STReP UbiSec&Sens of the EU Framework Program 6 for Research and Development (IST-2004-2.4.3). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the UbiSec&Sens project or the European Commission.

References

- 1) D. Dolev, A.C. Yao, "On the security of Public-Key Protocols," IEEE Transactions on Information Theory, 29(2):198-208, 1983
- 2) A. Weimerskirch, D. Westhoff, "Zero-Common Knowledge Authentication for Pervasive Networks," 10th Selected Areas in Cryptography, SAC'03, Springer-Verlag LNCS 3006, pp.73-87, Ottawa, Ontario, CA, August 2003
- 3) D. Westhoff, J. Girao, M. Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption," Key Distribution and Routing Adaptation, IEEE Transactions on Mobile Computing, in 2006
- 4) M. Acharya, J. Girao, D. Westhoff, "Secure Comparison of Encrypted Data in Wireless Sensor Networks," 3rd WiOpt, April 2005
- 5) J. Girao, D. Westhoff, E. Mykletun, T. Araki, "TinyPEDS: Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks," to appear at Elsevier Ad Hoc Journal.
- 6) E. Mykletun, J. Girao, D. Westhoff, "Re-visited: Public key based cryptoschemes for data concealment in wireless sensor networks," IEEE ICC, Turkey, May 2006

Authors' Profiles

Dirk WESTHOFF
Chief Researcher,
R&D Network Laboratories,
NEC Europe Ltd.
A member of the IEEE

Joao GIRAO
Research Staff,
R&D Network Laboratories,
NEC Europe Ltd.
A member of both the IEEE and the ACM

Amardeo SARMA
Manager,
R&D Network Laboratories,
NEC Europe Ltd.
A senior IEEE member

●The details about this paper can be seen at the following.
Related URL: <http://www.ist-ubiseconsens.org/>