

On the Feasibility and Meaning of Security in Sensor Networks

Zinaida Benenson and Felix C. Freiling

Department of Computer Science, RWTH Aachen University, Germany

Abstract. This paper is an invitation for the participants of “Fachgespräch Sensornetze” to discuss security issues in sensor networks in relation to particular projects in which the participants are involved. The central question to be discussed is: In what sense are the applications constructed by the participants secure? To structure the discussion, we give a taxonomy of adversary classes for sensor networks and give an overview over methods for securing sensor networks against these adversaries.

1 Introduction

Sensor networks provide unique opportunities of interaction between computer systems and the environment. Their deployment can be described at high level as follows: The sensor nodes measure environmental characteristics which are then processed in order to detect events. Upon event detection, some actions are triggered. This very general description applies to extremely security-critical military applications as well as to such benign ones (in terms of security needs) as habitat monitoring.

Considering the Internet as an example, it is extremely difficult to add security to systems which were originally designed without security in mind. The goal of security is to “protect right things in a right way” [1]. Thus, careful analysis is needed concerning which things to protect against which threats and how to protect them. This analysis is only possible in context of a particular class of applications. Therefore, we invite the workshop participants to start the analysis of *realistic* security requirements of their projects. In the following, we give a framework for this analysis.

We first give an overview of security goals in sensor networks, i.e., “what to protect” (Section 2). Then we describe the adversary classes (Section 3), i.e., “against whom to protect” and the existing solutions to various security problems (Section 4), i.e., “how to protect”. We outline open problems and summarize in Section 5.

2 Security Goals in Sensor Networks

A sensor network can be considered as a highly distributed database. Security goals for distributed databases are very well studied: The data should be accessible only to authorized users (Confidentiality), the data should be genuine (Integrity), and the data should be always available on the request of an authorized user (Availability). All these requirements also apply to the sensor networks and their users. Here, the distributed database,

as well as the sensor network, are considered as a single entity from the user's point of view. Therefore, we call these security issues *outside security*. To outside security belong, e.g., query processing [7, 11, 13], access control [3] and large-scale anti-jamming services [14].

The internal organization of a distributed database and of a sensor network are quite different. Outside security, as well as all other types of interactions between the user and the corresponding system, is based on the interactions between the internal system components (servers or sensor nodes, respectively). We call security issues for such interactions *inside security*. In sensor networks, inside security realizes robust, confidential and authenticated communication between individual nodes [9, 12]. This also includes in-network processing [5, 15], routing [4, 10] and in-network data storage [6].

Aside from necessitating the distinction between inside and outside security, sensor networks differ from conventional distributed databases in other obvious ways: A distributed database consists of a small number of powerful servers, which are well protected from physical capture and from network attacks. The servers use resource-demanding data replication and cryptographic protocols for inside and outside security. In contrast, a sensor network consists of a large number of resource-constrained, physically unprotected sensor nodes which operate unattended. Therefore, security measures for distributed databases cannot be directly applied to sensor networks. So even if a sensor network can be considered as a distributed system (e.g., as an ad hoc network), sensor networks have some additional features which make security mechanisms for distributed systems inapplicable. Apart from the obvious resource constraints, single sensor nodes are relatively unimportant for the properties of the whole system – at least, if the inherent redundancy of sensor networks is utilized in their design.

To summarize, security goals in sensor networks are similar to security goals in distributed databases (outside security) and distributed systems (inside security). However, many standard mechanisms (e.g., public key infrastructures or agreement protocols) are not applicable because they require too many resources or do not scale to hundreds or thousands of nodes. New approaches are needed to ensure security of sensor networks. These must exploit the natural features of sensor networks: inherent redundancy and broadcast communication.

Before discussing the protection techniques, we should determine against which threats to protect, which brings us to the adversaries.

3 Adversary Models for Sensor Networks

Adversary models should be determined with respect to applications. Who are adversaries and what goals do they have? A military sensor network has other security requirements than a network for habitat monitoring. The adversaries can be classified according to the following parameters: goals, interference, presence, and available resources. We treat each parameter in turn.

Goals. Which of the three classical security goals (Confidentiality, Integrity, Availability) does the adversary try to violate? If the data are valuable (legitimate users have to pay) or privacy relevant, the adversary would try to gain unauthorized access. If the

data are critical (building or perimeter security), the adversary would try to modify data, such that the alarm is not raised in case of intrusion. Also a denial-of-service attack can successfully disable the network (violating Availability).

Interference. A *passive* adversary eavesdrops on the network traffic and analyzes it (online or offline). *Active* adversaries come in several flavors:

- A *fail-stop* adversary attacks sensors such that they completely break down. The sensors can be destroyed or drained of energy.
- A *disturbing* adversary can try to partially disturb protocols, even if he does not have full control over any sensors. He can selectively jam the network, or fool some sensors into measuring fake data. For example, he can hold a lighter close to a temperature sensor [13] or re-arrange the topology of the sensor network by throwing sensors around.
- A *malicious* adversary can run arbitrary programs on a sensor node. This can be achieved by exploiting some software bug, or by probing out cryptographic keys and other secret information and then cloning the node. The problem of *node capture* is typical for a malicious adversary.

Presence. A *local* adversary can influence a small localized part of the network [3], for example he has one receiver which can only eavesdrop on several meters, or can manipulate only the sensor node which is the closest to him (for example, it is installed in his office). A *partially present* adversary is either mobile (a car with receiver driving around) or managed to install his own sensor nodes in the sensor field and coordinates them [2]. A *global* adversary is present in the whole network.

Available resources. There are several resource classes to consider: funding, equipment, expert knowledge, time. In the world of tamper resistance, the adversaries are divided into three classes: clever outsiders, knowledgeable insiders and funded organizations [1]. Commodity sensor networks are likely to be attacked by clever outsiders (who are probably just trying things out) and possibly by knowledgeable insiders, if a substantial gain from the attack can be expected.

Interesting issues arise in interplay of the above parameters. For example, a global adversary need not to be a funded organization. A hacker could subvert the entire sensor network by exploiting some software bug. Or, if a local adversary manages to capture a sensor node and read out its cryptographic keys, he can turn into a partially present or global adversary, depending on how many sensor nodes he is able to buy and deploy as clones of the captured node.

4 Protecting Sensor Networks

For passive adversaries, encryption techniques often suffice to ensure inside security. Symmetric key encryption techniques will be favored over asymmetric ones because of the computational advantage and the comparatively small key sizes. The problems arise in the setup phase of the network where shared secrets need to be distributed either by the manufacturer at production time or by clever protocols at deployment time [2, 8].

For stronger adversaries, active attacks like impersonation and node capture must be taken into account. Ideally, sensor nodes should be made tamper proof to prevent node capture, e.g., by applying technology known from smart cards or secure processing environments. There, memory is shielded by special manufacturing techniques which makes it more difficult to physically access the stored information [1]. Similarly, sensor nodes could be built in a way that they lose all their data when they are physically tampered with by unauthorized entities.

For large sensor networks, cost considerations will demand that sensor nodes are not tamper proof. Therefore, node capture must be taken into account. A first step to protect a sensor network from node capture against a local or partially present adversary is to use locally distributed protocols that can withstand the capture of a certain fraction of nodes in the relevant parts of the network. For example it is possible to devise access control protocols that work even if up to t out of n nodes in the communication range of the adversary are captured [3]. While these protocols can exploit broadcast communication, they are still relatively resource intensive.

A very general approach to counter node capture is to increase the effort of the adversary to run a successful attack. For example, data may be stored at a subset of nodes in the network and continuously be moved around by the sensors to evade the possible access by the adversary. This makes it harder for the adversary to choose which node to capture. In the worst case, the adversary must capture much more than t out of n nodes to successfully access the data in question.

A similar technique that exploits the inherent redundancy of a sensor network and shields against even global adversaries is to devise it as a virtual minefield. A certain fraction of sensors has special alerting software enabled which scans the communication in its vicinity and reacts to local and remote manipulations by issuing a distress signal in its environment or otherwise cause an unpleasant experience to the adversary. Thus, these sensors act as “mines” in the network which the adversary tries to avoid since capturing them needs more resources than capturing a normal sensor node. If it is not possible for the adversary to distinguish these special sensors from normal sensors, the ratio between the fraction of “mines” and the effort to capture them determines the incentive of the adversary to attack the system. For example, if 10% of the sensors are virtual mines and it takes 1000 times more effort to capture a mine than to capture a normal node, the adversary will waste a lot of resources if he needs to capture even a small subset of sensors without raising an alarm.

5 Summary and Open Problems

We have described security goals, adversary models and protection mechanisms which are relevant and specific for sensor networks. There are a lot of interesting problems and open questions in this area:

- *Realistic* adversary models should be derived with respect to existing and future applications. Here, experiences with GSM and WLAN security (and security failures) can be used as a guideline, but every application needs to define its own adversary model to be able to talk about security.

- As cross-layer integration is especially important for resource-constrained sensor nodes, careful design decisions must be taken concerning which security means to put into which layer. For example TinySec [9], a link layer encryption and message integrity protection mechanism, is integrated into the radio stack of MICA Motes.
- Building secure sensor networks, especially with respect to active adversary, remains a challenge. Can it be done by combining existing solutions, such as random key predistribution, secure routing, secure data aggregation, or would it be too expensive in terms of energy?

Overall, we speculate that probabilistic algorithms which exploit the redundancy of the sensor network to cause high effort for the adversary will be good candidates to establish security in such networks. In a sense, these algorithms mimic guerrilla tactics: evasion and disguise. They can be simple, yet unpredictable. However, their simplicity implies that they are not suitable to establish perfect security. The security goals of sensor networks will be probabilistic and depend on the strength of the adversary.

References

1. R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., 2001.
2. R. J. Anderson, H. Chan, and A. Perrig. Key infection: Smart trust for smart dust. In *ICNP*, pages 206–215, 2004.
3. Z. Benenson, F. C. Gärtner, and D. Kesdogan. An algorithmic framework for robust access control in wireless sensor networks. In *Second European Workshop on Wireless Sensor Networks (EWSN)*, January 2005.
4. J. Deng, R. Han, and S. Mishra. A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In *2nd IEEE International Workshop on Information Processing in Sensor Networks (IPSN 2003)*, April 2003.
5. T. Dimitriou and D. Foteinakis. Secure and efficient in-network processing for sensor networks. In *First Workshop on Broadband Advanced Sensor Networks (BaseNets)*, 2004.
6. A. Ghose, J. Grossklags, and J. Chuang. Resilient data-centric storage in wireless ad-hoc sensor networks. In *MDM '03: Proceedings of the 4th International Conference on Mobile Data Management*, pages 45–62. Springer-Verlag, 2003.
7. L. Hu and D. Evans. Secure aggregation for wireless networks. In *SAINT-W '03: Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*, page 384. IEEE Computer Society, 2003.
8. J. Hwang and Y. Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 43–52. ACM Press, 2004.
9. C. Karlof, N. Sastry, and D. Wagner. Tinysec: A link layer security architecture for wireless sensor networks. In *Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004)*, November 2004.
10. C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols*, September 2003.
11. B. Przydatek, D. Song, and A. Perrig. SIA: Secure information aggregation in sensor networks. In *ACM SenSys 2003*, Nov 2003.

12. H. Vogt. Exploring message authentication in sensor networks. In *Security in Ad-hoc and Sensor Networks (ESAS), First European Workshop*, volume 3313 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 2004.
13. D. Wagner. Resilient aggregation in sensor networks. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 78–87. ACM Press, 2004.
14. A. Wood, J. Stankovic, and S. Son. JAM: A mapping service for jammed regions in sensor networks. In *In Proceedings of the IEEE Real-Time Systems Symposium*, December 2003.
15. S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large-scale distributed sensor networks. In *Proceedings of the 10th ACM conference on Computer and communication security*, pages 62–72. ACM Press, 2003.