2011 Seventh European Conference on Computer Network Defense

Security in Wireless Sensor Networks

Andreas Larsson
Computer Science and Engineering,
Chalmers University of Technology
Email: larandr@chalmers.se

Philippas Tsigas
Computer Science and Engineering,
Chalmers University of Technology
Email: tsigas@chalmers.se

I. Introduction

A wireless sensor network is a network of small computers, sensor nodes, that can gather information via its sensors, do computations and communicate wirelessly with other sensor nodes. In general a wireless sensor network is an ad hoc network in which the nodes organize themselves without any preexisting infrastructure. Once in the area, the nodes that survived the deployment procedure communicate with the other nodes that happened to end up in its vicinity, and they set up an infrastructure.

Security is critical for many applications of sensor networks, just as for applications in other kinds of networks. Confidentiality and privacy is needed for sensitive, classified or proprietary information, e.g. medical data, sensitive information in civil security, industrial secrets or military information. It is important to be able to withstand attacks that aims to degrade the functionality of the network. Any kind of application can come under attack from someone that wants to disturb the network. For some applications it is critical to keep as much functionality as possible during an attack. Applications, e.g., that monitors restricted areas might have active attackers that have an interest in making the sensor network report erroneous information and the sensor network plays a critical role in maintaining security and/or safety of the facility.

Sensor networks are deployed in areas that is to be monitored. This usually implies that they are physically available for attackers. Furthermore, to feasibly deploy large number of nodes, they need to be inexpensive. Tamper-proof nodes are therefore often out of the question. The limitations in computing power, memory and battery makes many security algorithms inappropriate for use in sensor networks. This can limit the cryptography possibilities, especially for public key cryptography. Sensor networks often have very different traffic patterns than other networks. Information usually flows between the sensor nodes and the base station, or between nodes close to each other, but not between any pair of nodes in general. In addition, information is often aggregated on the way to decrease the total amount of needed traffic. The wireless medium makes it easy for an attacker to eavesdrop on the traffic, to jam communication or to inject messages into the network.

II. Secure services

Our research aims to provide high level networking protocols for sensor networks and/or ad-hoc networks that are both secure and self-stabilizing. Self-stabilization lets the networks recover from an arbitrary system configuration as long as system assumptions holds, e.g. after temporary faults or temporarily unheld assumptions.

Clock synchronization is an important service for many applications in sensor networks, such as mobile object tracking, detection of duplicates, and TDMA radio scheduling. The accuracy needs can be in the order of microseconds. In [1], we presented the first secure and self-stabilizing algorithm for clock synchronization in sensor networks that can withstand attacks from nodes inside the network. The core of the algorithm is a facility for nodes to exchange timestamps with each other in a secure and fault tolerant manner.

Self-organization is another key building block for ad hoc networks. One technique for such organization is to elect so called cluster heads that take certain responsibilities and that can be used to build up hierarchies. In [2], we presented the first distributed self-stabilizing (k,r)-clustering algorithm. A (k,r)-clustering provides every node in the network with k cluster heads within r communication hops. The algorithm rapidly elects enough cluster heads. A random process makes the network converge towards a local minimum, where no cluster head can be removed without violating the requirements. Multiple paths are used to improve security, availability and fault tolerance. This algorithm is suited for a network with synchronized clocks and reliable communication. In future work we aim to weaken these assumptions to be able to handle message loss and unsynchronized clocks.

References

[1] J.-H. Hoepman, A. Larsson, E. M. Schiller, and P. Tsigas, "Secure and self-stabilizing clock synchronization in sensor networks," *Theoretical Computer Science*, vol. 412, no. 40, pp. 5631–5647, 2011.

[2] A. Larsson and P. Tsigas, "A self-stabilizing (k,r)-clustering algorithm with multiple paths for wireless ad-hoc networks," in *Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS 2011)*, Minneapolis, Minnesota, USA, June 2011.

978-0-7695-4762-6/12 $26.00 © 2012 IEEE
DOI 10.1109/EC2ND.2011.13

CPS Conference Publishing Services