Security for Fixed Sensor Networks

Ning Hu, Randy K. Smith, Phillip G. Bradford
Dept. of Computer Science
The University of Alabama
Tuscaloosa, Alabama 35487-0290
{nhu, rsmith, pgb}@cs.ua.edu

ABSTRACT

Sensor networks consist of resource-constrained sensors operating in a variety of environments. Given the severe constraints on these sensors, it is a particularly challenging problem to choose and design valid security protocols for such networks. This problem has recently given rise to new research addressing the security issues. This paper presents an overview of the important works, specifically the new mechanisms and protocols, which have been introduced or are still under development in this area.

1. OVERVIEW

Sensor networks are an emerging wireless computing technology for monitoring a variety of environments in scientific, military, medical, and other critical applications. Such networks comprise collections of wireless micro-sensors. These sensors are deployed within a predetermined geographical area to self-organize into an ad hoc wireless network to gather and aggregate data. These sensor nodes are characterized by severely limited resources in terms of memory size, computational power, and bandwidth, and even energy. The SmartDust Node [6], for example, only possesses an 8-bit CPU, an 8KB instruction flash memory, and a bandwidth of 10 Kbps. To support secure networking with such tiny devices is a real challenge. The conventional security measures, e.g. asymmetric keys, intended for larger communication devices, such as PDAs, are not readily transferable to resource-constrained sensor nodes [3].

The ad hoc nature of sensor networks makes them particularly vulnerable to interception, intrusion and service deprivation. Without encryption and integrity checking, the contents of a broadcast message is subject to eavesdropping and tampering. Without authentication, an attacker can easily inject malicious code or false data into the network by either subverting a good node or inserting a bad node. Still worse, the attacker can inflict sleep torture on an energy constrained node by engaging it in unnecessary communication work to quickly drain its battery power. The effects of these attacks can be dramatic: a compromised node in an airport surveillance system may pose serious threats to flight safety. In military applications, a sensor node captured by the enemy troops may be reverse engineered and become an instrument for mounting counterattacks. In either context, depriving the power of a few crucial nodes may lead to the communication breakdown in the entire network.

Given the serious threats to sensor networks, and the lack of effective countermeasures due to resource constraints of sensors, recent research [2, 4, 5, 7, 1, 8] has tailored security mechanisms and protocols for these networks. The implication of security in sensor networks is mainly quadruple, i.e. confidentiality (privacy of communication), authenticity (trustworthiness of a source), integrity (non-modification in transit), and freshness (no replayable messages) [5, 1, 8]. Consequently, most of the aforementioned works [2, 4, 5, 7, 1, 8] were developed along these four lines with indispensable considerations for resource-security trade-off in sensor networks.

Chen *et al.* [2] are among the first to propose a security model for communication between the base station and sensor nodes in wireless sensor networks. Perrig *et al.* [4, 5] customize a more complete suite of security protocols, collectively known as SPINS (Security Protocols for Sensor Networks), for a similar network infrastructure. Avancha *et al.* [1, 8] follow Perrig *et al.*'s research with a security protocol for base-station-to-node communication. The three studies all give prominence to the base station in their attempts to secure the sensor network. Alternately, Slijepcevic *et al.* [7] propose a layered architecture that selectively applies protection schemes according to the types of data sent through the network. By so doing, they seek to balance security implementations with resource consumption. The remainder of this paper outlines these four important works.

2. CHEN *ET AL*'S WORK

Chen *et al.* [2] propose two security protocols for the massive deployment of sensor networks for real-world applications. The first protocol is *base station to mote confidentiality and authentication.* It prescribes that an efficient shared-key algorithm, e.g. RC5, be used to guarantee the authenticity and privacy of information. The choice of RC5 over a public key algorithm is owing to its low memory consumption and high encryption performance, suitable for implementation on a sensor node. The second protocol is *source authentication*, which implements a hash chain function similar to that used by TESLA (Timed Efficient Stream Loss-tolerant Authentication) [3] to achieve *mote* authenti-

ACMSE '04, April 2-3, 2004, Huntsville, Alabama USA
Copyright 2004 ACM 1-58113-870-9/04/04 ...$5.00.

cation.

Although their work establishes a secure channel between the base station and sensor nodes, it provides no security for inter-node communication. The lack of authentication among intermediate nodes along the path of a message transfer gives rise to insecure data aggregation among sensor nodes. Furthermore, TESLA is originally designed to support secure transactions among workstations abounding in resources. It is not the best fit for networks made of resource-starved sensor nodes. A sensor network version of the protocol, called μTESLA (micro-TESLA), is proposed in the SPINS model[4, 5].

3. SPINS

SPINS is a collection of security protocols developed by Perrig *et al.* for sensor networks [4, 5]. The model integrates two major modules, i.e. SNEP (Secure Network Encryption Protocol) and μTESLA. SNEP supports end-to-end security and μTESLA authenticated broadcast. To lower communication overhead, SNEP uses a shared counter for a pair of sender and receiver nodes. To reduce storage, μTESLA limits the size of a MAC entry to only 8 bytes long, and discloses a key once per epoch. Computation costs are also kept low by using only symmetric cryptography. To conserve node resources, μTESLA stores the key chain in a base station and broadcasts data through the station.

The model leaves open quite a few unresolved security issues, such as information leakage, compromised nodes and DoS (denial-of-service) attacks (see Section 7 of [5] for details). Additionally, the validity of the protocols are based on a few assumptions concerning the network architecture. For example, the model assumes a static network topology and an ideal base station, always dependable and inexhaustible in resources. Furthermore, the model requires that the base station unicast to each node a key disclosure schedule, at bootstrap time. The resulting communication overhead causes the problem of scalability for bandwidth-constrained sensor networks.

4. AVANCHA *ET AL*'S WORK

The system proposed in [1, 8] utilizes the base station as the major authenticator of the sender of incoming packets for their secuiry model. The base station is assumed to work in perfect conditions, and is capable of detecting aberrant nodes in the network. It achieves this by maintaining maintains live statistics regarding node activities, such as most recent DTGs, number of corrupted messages, and number of route failures. Futhermore, the model descends to the packet level to implement security mechanisms. A data packet is encrypted with shared keys for source authentication and data integrity, and contains a DTG field to ensure data freshness. Based on simulation results (Section 5 of [1, 8]), Avancha *et al.* claim that their security model contributes to energy conservation in the sensor network.

5. LAYERED SECURITY MODEL

Slijepcevic *et al.* take a layered approach to the trade-off of security and resource constraints for sensor networks. Network data is ranked into three security levels by protection priority. At the highest level is the mobile application code, which is most crucial for network operations, but least frequently transferred. The information regarding the physical locations of sensors receives the secondary level of protection in order to reduce the high encryption overhead due to the frequent transmission of such information. The application data is considered the least sensitive and most frequent. Subsequently, it is relegated to the lowest level of protection.

The layered approach provides a possible solution to the efficient management of limited resources for sensor network security. Nevertheless, the applicability of this model is constrained by the nature of data under protection. In fact, application data is not always the least important, especially in military contexts. Some applications may even require its data to be uncompromisible to adversaries. Accordingly, such data ought to be promoted to a higher security level. Unfortunately, the resulting higher overhead coupled with the high frequency of the data will probably take a toll on resources.

6. REFERENCES

[1] Sasikanth Avancha, Jeffery Undercoffer, Anupam Joshi, John Pinkston (2003): "Secure Sensor Networks for Perimeter Protection," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, **43(4)**, 421–435, 2003.

[2] Mike Chen, Weidong Cui, Victor Wen, Alec Woo (2000): "Security and Deployment Issues in a Sensor Network," http://www.cs.berkeley.edu/ wdc/classes/cs294-1-report.pdf, December 2000.

[3] Adrian Perrig, Ran Canetti, J. D. Tygar, Dawn Xiaodong Song (2000): "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *IEEE Symposium on Security and Privacy*, May 2000.

[4] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler (2001): "SPINS: Security Protocols for Sensor Networks," *Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001*, July 2001.

[5] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler (2002): "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, Vol.8, 521-534, 2002.

[6] Kris S. J. Pister, Joe M. Kahn, Bernhard E. Boser (1999): "Smart Dust: Wireless Networks of Millimeter-Scale Sensor Nodes," *Highlight Article in 1999 Electronics Research Laboratory Research Summary*, 1999.

[7] Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, Mani B. Srivastava (2002): "On Communication Security in Wireless Ad-Hoc Sensor Networks," *Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02)*, 139-144, 2002.

[8] Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi, John Pinkston (2002): "Security for Sensor Networks," *CADIP Research Symposium*, 2002.