Forum Session:
Security for Wireless Sensor Networks

David Carman
Network Associates Laboratories
David_Carman@nai.com

Daniel Coffin
BBN Technologies
dcoffin@bbn.com

Bruno Dutertre
SRI International
bruno@sdl.sri.com

Vipin Swarup
The MITRE Corp.
swarup@mitre.org

Ronald Watro
BBN Technologies
rwatro@bbn.com

Abstract

Wireless networks of low-power sensing devices are poised to become a ubiquitous part of the computing landscape. Proposed applications of these networks range from health care to warfare. The challenge for the information security community is to develop the common security services (confidentiality, integrity, etc.) for sensor networks in a manner that meets the very strict resource constraints of these devices. This forum will describe a broad range of on-going research efforts in order to acquaint the general information security community with the issues and concerns of sensor net security.

1. Overview

The emergence of low-power sensor networking has been propelled by the convergence of advances in several fields, including nano-technology, Micro Electronic Mechanical Systems (MEMS), radio frequency communications, and microprocessors. These research efforts are culminating in programs such as the UC Berkeley "Smart Dust" project, which recently announced a sensor/transceiver chip called Spec just 5 mm^2 in size and requiring one thousand times less power than a conventional cell phone [1]. Ad hoc networks of such miniaturized sensor/transceiver units create a powerful tool for information gathering. These networks may include relatively more powerful base stations or relay points that serve to connect the sensor network to the outside world. In other instances, the sensor nodes themselves serve as dynamic relay points. Current commercial sensor/transceiver devices from companies such as Crossbow, Dust, Ember, and Sensicast Systems provide custom communication stacks and the beginning of hardware support for symmetric encryption. Efficient key management, minimizing use of communication and computation, remains a critical challenge.

Security research for sensor networks takes several forms:

- **New, more efficient cryptographic algorithms and security protocols**.
  Efficient versions of public key cryptography (such as the NTRU algorithms [2]) and broadcast authentication protocols (such as µTESLA [3]) have been devised.

- **Asymmetric algorithms and protocols.**
  Security services have been designed to place the primary computational and communication burden on external entities and/or relay devices rather than on sensor nodes.

- **Integration of security into applications.**
  The computing infrastructure of miniaturized devices is often much flatter than conventional devices, avoiding layers of networking protocols and application functionality for performance reasons. This approach requires security to be deployed at higher abstraction levels, since a generic security service is too costly.

- **Limited acceptance of vulnerabilities.** Sensor net security services have been designed to accept specific vulnerabilities when they are compatible with application goals and provide performance advantages. Examples are reduced computational rounds in symmetric encryption computation and key management protocols that rely on an initially unauthenticated message.

The forum participates will describe their own efforts to create and deploy security services in ad hoc networking environments and their vision for the future.

2. Forum Participants

The follow individuals are expected to participate in the forum session.

David Carman is a Principal Cryptographic Engineer at Network Associates Laboratories, the security research division of Network Associates. He is currently the Tactical Information Protection industry technical area lead for the Army Research Laboratory's Communication and Networking Collaborative Technology Alliance and the industry principal investigator for the Highly Efficient Security Services and Infrastructure Task. Recently, he designed and implemented the security for the Army Research Laboratory's "Blue" Sensor Network Radio. Mr. Carman began practicing cryptography in 1986 at the National Security Agency and has since been the principal investigator for numerous security efforts.

Daniel Coffin is a Senior Engineer in the Mobile Networking Systems Department at BBN Technologies where he develops networking solutions for mobile ad-hoc wireless systems. Prior to BBN, Mr. Coffin worked at NTRU Cryptosystems on efficient public key technology for embedded environments as well as symmetric and asymmetric authentication protocol development. In earlier work, at MIT Lincoln Laboratory, he was the Principal Investigator for ad-hoc wireless sensor routing algorithms in the DARPA SensIT program.

Dr. Bruno Dutertre is a Senior Computer Scientist in the System Design Laboratory at SRI International. He is currently the Principal Investigator for SRI's Intrusion Tolerance project in the DARPA IXO NEST program. Dr. Dutertre's NEST project is developing low-cost key exchange and authentication protocols that rely exclusively on symmetric key cryptography. This includes "bootstrapping protocols" that enable devices to establish secure local links with their neighbors in a short time period after the network is deployed.

Dr. Vipin Swarup is a Principal Engineer in the Security and Information Operations Division at MITRE. He is currently the principal investigator of a MITRE project developing context-sensitive security mechanisms for mobile devices. In the past, Dr. Swarup has been the principal investigator of research projects in intrusion detection, security guards, mobile agent security, and type theory.

Dr. Ronald Watro is a Division Engineer in the Information Security Department at BBN Technologies. He is currently the Principal Investigator for BBN's Lightweight Security project in the DARPA IXO NEST program. In addition to DARPA work, Dr. Watro is involved with other government agencies developing the secure global information grid. In his previous position at MITRE, Dr. Watro worked in many aspects of information security, including automated reasoning and formal design verification. In earlier work, Dr. Watro developed distributed, fault-tolerant algorithms for asynchronous communication environments.

References

1. "Spec takes the next step …", http://www.cs.berkeley.edu/~jhill/spec/index.htm

2. J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," in *Algorithmic Number Theory (ANTS III),* J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998.

3. A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Proceedings of MOBICOM*, 2001.