Problems of Security in Ad Hoc Sensor Network

Petr Hanáček*
hanacek@fit.vutbr.cz

Abstract: The paper deals with a problem of secure communication between autonomous agents that form an ad hoc sensor wireless network. The paper is focused on the problem of communication in the Bluetooth wireless network, but the model should be general enough to support also other kinds of wireless short-range networks, e.g. networks with infrared communication, WiFi communication, and proprietary radiomodem communication.

Key Words: Sensor networks, Bluetooth, ad-hoc networks, tamper resistance.

1 Introduction

In the past years one of the most evolving part of computing and communication has been wireless networks technology. Wireless networks range from very big networks (e.g. satellite networks, cellular networks), middle-size networks (e.g. metropolitan networks), to small networks (e.g. personal wireless networks). One kind of small network is so called sensor network. Especially large-scale networks of wireless sensors are becoming increasingly available. Advances in hardware technology and radio engineering have led to dramatic reductions in size, power consumption and cost for circuitry of these networks. This has enabled very compact, autonomous and mobile nodes, each containing one or more sensors, computation and communication capabilities, and a power supply. Communication can now take the form of wired, short-range radio links, infrared, optical, and various other techniques. Sensors can detect light, heat, position, acceleration, movement, and so on.

A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. Some examples of wireless ad hoc sensor networks are the following [10]:

- Military sensor networks to detect and gain as much information as possible about enemy movements, explosions, and other phenomena of interest.
- Sensor networks to detect and characterize chemical, biological, radiological, and explosive material.
- Sensor networks to detect and monitor environmental changes in plains, forests, oceans, etc.
- Wireless traffic sensor networks to monitor vehicle traffic on highways or in congested parts of a city.
- Wireless surveillance sensor networks for providing security in shopping malls, parking garages, and other facilities.
- Wireless parking lot sensor networks to determine which spots are occupied and which are free.

* Doc. Dr. Ing., Faculty of Information Technology, Technical University of Brno, Božetěchova 2, CZ-612 66 Brno

The basic characteristic of ad-hoc sensor network is the communication among nodes of network without any pre-existing network structure or infrastructure (Figure 1).

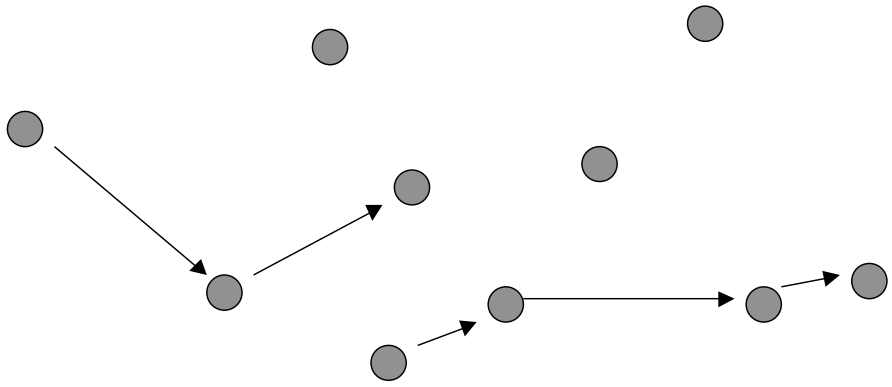

Fig. 1. Ad-hoc network – messages propagate through network using intermediate nodes

2 Cell architecture

In these networks, each node may contain a number of sensors, such as mechanical, optical, acoustic, infrared, etc. These nodes may be organized in clusters such that a locally occurring event can be detected by most of, if not all, the nodes in a cluster. Each node may have sufficient processing power to make a decision, and it will be able to broadcast this decision to the other nodes in the cluster. One node may act as the cluster master, and it may also contain a longer-range radio using a protocol such as WiFi or Bluetooth. Generally the cell of the network consists of two subsystem – computing subsystem and communication subsystem.

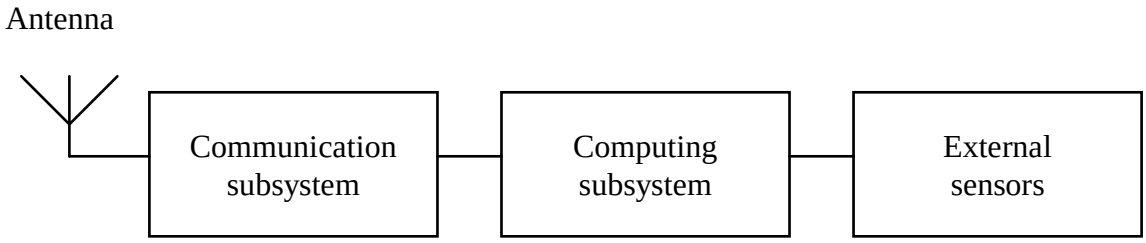

Fig. 2. General structure of node

3 Security threats for ad hoc networks

Computing in sensor networks poses problems to networking because the changing physical location requires continuous reconfiguration of the data links. If connectivity cannot be always maintained it also requires applications to handle extended off-line periods. The code in sensor network nodes generally runs in untrusted environment. Running code in untrusted environment means that programs or program fragments are executed on computers that could have different interests than an author of the code. Such programs are also called mobile code.

Mobile code however, suffers from considerable security problems. From the security point of view there is a number of threats for the sensor network. Main threats include:

- Eavesdropping of communication is the basic attack. The attacker can deduce from eavesdropped messages all available information about the sensor network, including security relevant information and position of individual nodes.
- Replay of messages is common attack if the attacker is not able to break the cryptographic protection of messages but is able to re-send previously sent genuine messages.
- Disturbing the communication by injecting noise in the radio channel is a simple attack that can be used to make the communication within the network impossible. This attack could be made more difficult by using spread spectrum radio channels.
- Masquerading the node of sensor network means that the attacker produces its own network node and attempts to connect this bogus node to existing network.
- Tampering with the node computer means that the attacker is able to use direct logical or physical manipulation with the node to change the behaviour of the node and, consequently perform further attacks on the rest of the network. The attacker also can try to acquire the cryptographic keys stored in the node computer.

4 Possible countermeasures

The security countermeasures fall into three areas – protection of radio channel, protection of messages, and protection of node hardware.

4.1 Spread spectrum

Basic countermeasure against eavesdropping, replay, and disturbing is so called spread spectrum technique. This countermeasure is often implemented as a frequency hopping mechanism. This technique quickly changes the radio frequency during data transmission to make attack to on-the-air communication more difficult. The frequency hopping also makes the localization of the network nodes more difficult and thus minimizes the threat of disclosing node position.

4.2 Cryptographic protection

The role of cryptography is very important in the design of sensor networks that should work in hostile environment with different threats. The application of cryptographic mechanisms can help achieve objectives such as confidentiality, data integrity, authentication, and non-repudiation. The cryptographic mechanisms used in sensor networks systems include secret key encryption/decryption, one-way hash functions, challenge-response cryptographic protocols, and digital signatures.

Confidentiality is typically achieved by using secret key encryption methods. Although it can also be done by applying asymmetric algorithms, the performance and price advantages of the symmetric algorithms are generally preferred. Data integrity and authentication are achieved by applying well-known hashing and MAC algorithms, such as CBC-MAC and SHA.

4.3 The role of tamper resistant hardware

The concept of tamper resistant hardware is tightly coupled with the concept of reference monitor. The reference monitor was defined in [1] and was standardized in [2]. The reference monitor concept was found to be an essential element of any system that would provide

multilevel secure computing facilities and controls. Reference monitor is also a heart of the most of cryptographic modules using secret-key cryptography. A usual implementation of reference monitor is a reference validation mechanism, so we will define the reference monitor in this implementation (see [2]). Reference validation mechanism as "an implementation of the reference monitor concept that validates each reference to data or programs by any user (program) against a list of authorized types of reference for that user." Three design requirements that must be met by a reference validation mechanism are:

- The reference validation mechanism must be tamper proof.
- The reference validation mechanism must always be invoked.
- The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured.

The implementation of this concept in described system is done by using the secure microcontroller as a computing subsystem. The used microcontroller should always have such physical and logical properties that it complies to the three above conditions. The conditions are met in following ways:

- The reference validation mechanism is tamper proof because of physical properties of the used microcontroller, which is designed as secure hardware that is resistant against physical, electrical, electro-magnetic, and chemical tampering.
- The reference validation mechanism is invoked because of communication protocol that is the only way to communicate with the microcontroller.
- The reference validation mechanism is small enough to be subject to analysis and tests, because of simplicity and standardization of the communication protocol that is used.

For the long time the tamper resistance of security computers (e.g. smartcards and security processors) was accepted without discussion. It was known, those large companies, like Intel or IBM, can successfully reverse-engineer complex chips, but everybody thought that this kind of attack is far beyond abilities of general attackers. The problem of evaluating the level of tamper resistance offered by a given product has been neglected by the security research community. It was discovered in the past that attacks on tamper resistance are possible also by small companies and even by individuals (see [9]). The tamper resistance of smartcards and security processors has to be now closely examined product by product to discover possible vulnerabilities.

4.4 Threat coverage by countermeasures

In the following table is clearly presented the coverage of threats (possible hostile action) by corresponding security countermeasures. Every threat is covered at least by one security countermeasure, but could be also covered by more countermeasures.

Hostile action	Basic security measure	Additional security measure
Eavesdropping	Traffic encryption – confidentiality	Frequency hopping
Masquerading	Traffic encryption – authentication, integrity	
Replay	Traffic encryption – authentication, integrity	
Theft	Tamper resistant hardware	
Noise, disturbing	Frequency hopping	

5 Communication system model

Used model of communication system is designed with the intention of simulation of various attacks and protection against these attacks. Generally the sensor network nodes use radio frequency communication, so broadcast is the basic communication primitive. This primitive is not very suitable for message routing; so on this primitive is built a communication primitive using bidirectional links. This communication model has also another advantage – it allows using commercial off-the-shelf radio communication modules, such as Bluetooth or WiFi that support bidirectional links.

Although both Bluetooth and WiFi communication standards support cryptographic protection of transmitted messages, this feature is not used in sensor networks. The security mechanisms of these standards support only security of transmission between two nodes, but not the security of messages transferred through number of nodes, that could be potentially untrusted.

The security of transmitted data is provided on the packet level (because of dynamic routing). All packets are cryptographically protected by symmetric secret key, shared between sending node and receiving node. The key is stored in tamper resistant hardware. This shared key allows mutual authentication of communicating nodes.

Confidentiality and integrity is provided by symmetric encryption. All packets are encrypted (except routing information) using symmetric cipher and secret key, shared between sending node and receiving node.

6 Conclusions

Sensor networks have the potential to provide important benefits to data gathering in hostile environment if implemented with appropriate security. These systems cannot be made fully secure against all types of attack. Determining the appropriate level of security for a particular system should involve consideration of the magnitude of potential risks, the cost of implementing varying levels of security and the impact on the functionality of the whole system. The described project is in this time in the phase of the designing and testing various components of the system using different approaches.

This work has been supported by the Grant Agency of Czech Republic grants No. 102/04/0871 "Information System Security - Research of Attacks on Tamper-Resistant Cryptographic Hardware".

References

1. Anderson, J. P. Computer Security Technology Planning Study, ESD-TR-73-51, vol. I, ESD/AFSC, Hanscom AFB, Bedford, Mass., October 1972 (NTIS AD-758 206).
2. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STDm December 1985, US Department of Defense, December 26, l985
3. Miller, B. A, Bisdikian, C., Bluetooth Revealed, Prentice Hall, 2001
4. IETF, Manet Group, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, 2001, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-05.txt
5. IETF, Manet Group, Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification, 2001, http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-03.txt
6. IETF, Manet Group, Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks, 2001, http://www.ietf.org/internet-drafts/draft-ietf-manet-lanmar-00.txt
7. Marinkovic, G., Beric, A., Radovanovic, A.: Ad-hoc Multihop Sensor Network, Computer Society International Design Competition, 2001
8. Sander, T., Tschudin, Chr.: Towards Mobile Cryptography, In the Proceedings of the 1998 IEEE Symposium on Security and Privacy.
9. Anderson, R.J., Kuhn, M.: Tamper Resistance - a Cautionary Note, in The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp 1-11
10. NIST, Advanced Networks Technologies Division, http://w3.antd.nist.gov/wahn_ssn.shtml