SETIT 2007
4th International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications
March 25-29, 2007 – TUNISIA

A Survey on Wireless Sensor Networks Security

Mona Sharifnejad*, Mohsen Sharifi**,
Mansoureh Ghiasabadi* and Sareh Beheshti*

* *ARAK Islamic AZAD University*
m-sharifneiad@iau-arak.ac.ir
m-ghias@ iau-arak.ac.ir
s-beheshti@ iau-arak.ac.ir

** *Computer Engineering Department*
Iran University of Science and Technology
msharifi@iust.ac.ir

Abstract: Computer security has always been a great concern and all sorts of solutions have traditionally been sought to encounter existing security breaches in various fields that deploy computational machines. This concern gets more and more critical upon introduction and consequent wide deployment of new technologies such as wireless sensor networks. Given the severe resource constraints of the constituent elements of these networks, traditional computer security solutions are not applicable here. Therefore, much research has focused on how to secure wireless sensor networks ever since their deployment in mission-critical domains. This paper presents a concise survey on the obstacles and the requirements for wireless sensor networks security, classifies important attacks and finally lists their corresponding defensive measures.
Key words: Wireless Sensor Networks, Security, Attacks

INTRODUCTION

In future, there will be thousands to millions of small sensors forming self-organizing wireless networks. These sensor networks are characterized by limited power and energy supplies, low bandwidth, small memory size, unreliable communication (e.g. unreliable transfer, conflicts and latency) and unattended operation. Therefore traditional security techniques in computer networks are not suitable and useful for wireless sensor networks.

Researchers have begun focusing on building a sensor trust model to solve the problems beyond the capability of cryptographic security and they have tried to address the challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers.

In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks. Furthermore, due to the inherent unattended feature of wireless sensor networks, physical attacks to sensors play an important role in the operation of wireless sensor networks.

The reminder of this paper is organized as follows. Section 2 details the requirements for the sensor network security. Section 3 categorizes major attacks in sensor networks, and Section 4 presents the corresponding defensive measures. Finally, Section 5 concludes the paper.

1. Security Requirements

In this section, we formalize the security properties required by sensor networks, and show how they are directly applicable in a typical sensor network.

1.1. Data Authentication

Authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). At the same time, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, *data authentication* allows a receiver to verify that the data really was sent by the

claimed sender.

1.2. Data Confidentiality

A sensor network should not leak sensor readings to neighboring networks. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality.

1.3. Data Integrity

The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

1.4. Data Freshness

A key establishment process ideally should guarantee its participants that each shared key (session key) is fresh. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed.

Key establishment provides one of two forms of freshness guarantee. The weaker form, which provides partial message ordering, ordering, but carries no delay information, and strong form, which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network.

1.5. Self Organization

A wireless sensor network requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well.

If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating.

1.6. Availability

To ensure the availability of message protection, the sensor network should protect its resources (i.e., sensor nodes) from the unnecessary processing of key management messages in order to minimize energy consumption and extend the life of the network.

Key management functions should not limit the availability of the network and not create single points of failure such as a centralized key management node for all network-wide security.

1.7. Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pairwise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. [8], proposes a set of secure synchronization protocols for sender-receiver (pairwise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

1.8. Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non-secured location information by reporting false signal strengths, replaying signals, etc.

There are some techniques in this area. For example VM (verifiable multilateration) [24] and SeRLoc (Secure Range-Independent Localization) [13].

In multilateration, a device's position is accurately computed from a series of known reference points. Authenticated ranging and distance bounding are used to ensure accurate location of a node.

In SeRLoc, a sensor computes its location by listening for the beacon information sent by each locator. The beacons include the locator's location. Using all of the beacons that a sensor node detects, a node computes an approximate location based on the coordinates of the locators. All beacons transmitted by the locators are encrypted with a shared global symmetric key that is pre-loaded to the sensor prior to deployment. Each sensor also shares a unique symmetric key with each locator. This key is also pre-loaded on each sensor.

1.9. Scalability

Distributed Sensor Networks (DSNs) have on the order of 10 to 10,000 nodes, of which at most a small number (< 10) of these nodes are energy rich super nodes or gateway nodes. Large DSNs cannot utilize a keying scheme that has poor scaling properties (either in terms of energy cost or latency) for establishing and maintaining a key for the DSN as a whole or for some large subset of nodes.

Most group keying schemes have some cost related parameter (number of encryption operations, number of bits received) that grows rapidly with increasing group size. For lightly used groups, or groups where the members often modify messages rather than just forwarding them, it is more efficient to use multiple smaller subgroups (with different group keys), and simply re-encrypt messages when they are

forwarded from one subgroup to another. This approach is especially attractive when transmission energy costs are more important than computational costs.

1.10. Accessibility

End-to-end confidentiality of sensor data should not be performed since it prevents sensor data fusion by intermediate nodes from taking place. To provide intermediate node accessibility, a key management scheme must establish keying relationships, either directly or transitively, with all potential intermediate nodes between all potential sensing nodes and all potential destination nodes. Direct keying relationships between all potential sensing, intermediate, and destination nodes may be accomplished by having a single network-wide key for all nodes. Transitive keying relationships allow intermediate nodes along the multi-hop communications path to decrypt and verify received data via one key, and use another key to re-encrypt and authenticate data to be forwarded. Instead of creating a single network-wide key, transitive relationships allow much smaller groups to establish keying relationships.

1.11. Flexibility

Sensor networks will be used in dynamic battlefield scenarios where environmental conditions, threat, and mission may change rapidly. Changing mission goals may require sensors to be removed from or added to an established sensor node. Furthermore, two or more sensor networks may be fused into one, or a single network may be split in two .Key establishment protocols must be flexible enough to provide keying for all potential scenarios a sensor network may encounter. Protocols that require knowledge of what other nodes will be co-deployed are discouraged, whereas protocols with minimal preconceptions are encouraged.

2. Types of Attacks

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways: Denial of service attacks, Sybil attacke, Traffic analysis, Privacy violation, Physical attaché and so on.

2.1. The Sybil Attacks

The Sybil attack is defined as a “malicious device illegitimately taking on multiple identities” [15]. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks [7]. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection.

2.2. Denial of Service Attacks

A Type of standard of Denial of service attacks on wireless sensor networks is jamming a node or set of nodes. The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently.

Denial of service Attacks can also be made on the link layer itself. One possibility is that an attacker may simply intentionally violate the communication protocol [30] and continually transmit messages in an attempt to generate collisions. Such collisions would require the retransmission of any packet affected by the collision. Using this technique it would be possible for an attacker to simply deplete a sensor node’s power supply by forcing too many retransmissions.

The rooting layer and transport layer are also susceptible to attack. [26]

2.3. Physical Attacks

Physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker [25].

2.4. Node Replication Attacks

Conceptually, a node replication attack is quite simple: an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node. A node replicated in this fashion can severely disrupt a sensor network’s performance: packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor and can also insert the replicated node into strategic points in the network [17]. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

2.5. Privacy Violation by Attacks

Some of the more common attacks [9] against sensor privacy are:

- **Monitor and Eavesdropping.** By listening to the data, the adversary could easily discover the communication contents.
- **Traffic Analysis.** Traffic analysis typically combines with monitoring and eavesdropping. An increase in the number of transmitted packets between certain nodes could signal that a specific sensor has registered activity.
- **Camouflage**. Adversaries can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can masquerade

as a normal node to attract the packets, then misroute the packets, e.g. forward the packets to the nodes conducting the privacy analysis.

2.6. Traffic Analysis Attacks

Wireless sensor networks are typically composed of many low-power sensors communicating with a few relatively robust and powerful base stations. It is not unusual, therefore, for data to be gathered by the individual nodes where it is ultimately routed to the base station. Often, for an adversary to effectively render the network useless, the attacker can simply disable the base station. To make matters worse, Deng *et al.* demonstrate two attacks that can identify the base station in a network (with high probability) without even understanding the contents of the packets (if the packets are themselves encrypted) [5].

3. Defensive Measures

There are many Defensive Measures for protecting the sensor networks from attacks: key establishment in wireless sensor networks, defending against DoS attacks, secure broadcasting and multicasting, defending against attacks on routing protocols, combating traffic analysis attacks, defending against attacks on sensor privacy, intrusion detection, secure data aggregation, defending against physical attacks, and trust management.

3.1. Key Establishment

Most of the traditional techniques, however, are unsuitable in low power devices such as wireless sensor networks. Key exchange techniques use asymmetric cryptography, also called public key cryptography. Two of the major techniques used to implement public-key cryptosystems are RSA and elliptic curve cryptography (ECC) [21].

The LEAP protocol takes an approach that utilizes multiple keying mechanisms. Their observation is that no single security requirement accurately suites all types of communication in a wireless sensor network. Therefore, four different keys are used depending on whom the sensor node is communicating with [29].

Huang *et al.* [11] propose a hybrid key establishment scheme that makes use of the difference in computational and energy constraints between a sensor node and the base station. They posit that an individual sensor node possesses far less computational power and energy than a base station.

3.2. Defending against DoS Attacks

One strategy in defending against the classic jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion. [26] Describes a two phase approach where the nodes along the perimeter of the jammed region report their status to their neighbors who then collaboratively define the jammed region and simply route around it.

To overcome the transport layer flooding denial of service attack, in [2] suggests that a server should always force a client to commit more resources up front than the server. This strategy would likely be effective as long as the client has computational resources comparable to those of the server.

3.3. Secure Broadcasting and Multicasting

Multicasting and broadcasting techniques have been used to reduce the communication and management overhead of sending a single message to multiple receivers. In both a wired and wireless network this is done using cryptography.

Di Pietro *et al.* describe a directed diffusion based multicast technique for use in wireless sensor networks that also takes advantage of a logical key hierarchy [18]. In directed diffusion, a query is transformed into an interest (due to the data-centric nature of the network). The interest is then diffused throughout the network and the network begins collecting data based on that interest.

In [12] suggests a routing-aware based tree where the leaf nodes are assigned keys based on all relay nodes above them. They argue that their technique, which takes advantage of routing information, is more energy efficient than routing schemes that arbitrarily arrange nodes into the routing tree.

3.4. Defending against Attacks on Routing Protocols

There is a great need for both secure and energy efficient routing protocols in wireless sensor networks as attacks such as the sinkhole, wormhole and Sybil attacks demonstrate [15].

Tanachaiwiwat, *et al.* presents a novel technique named TRANS (Trust Routing for Location Aware Sensor Networks). The TRANS routing protocol is designed for use in data centric networks. It also makes use of a loose-time synchronization asymmetric cryptographic scheme to ensure message confidentiality [23].

One particular challenge to secure routing in wireless sensor networks is that it is very easy for a single node to disrupt the entire routing protocol by simply disrupting the route discovery process. In [16], proposes a secure route discovery protocol that guarantees. This scenario is somewhat similar to the TRANS protocol mentioned above. The security relies on the MAC (message authentication code) and an accumulation of the node identities along the route traversed by a message.

3.5. Detecting Node Replication Attacks

Parno, et al. describes two algorithms: randomized multicast, and line-selected multicast. Randomized multicast is an evolution of a node broadcasting strategy. In the simple node broadcasting strategy each sensor propagates an authenticated broadcast message throughout the entire sensor network. Any node that receives a conflicting or duplicated claim revokes the

conflicting nodes [17].

Randomized multicast improves upon the insecurity of deterministic multicast by randomly choosing the witnesses. In the event that a node is replicated two sets of witness nodes are chosen.

The line-selected multicast algorithm seeks to further reduce the communication costs of the randomized multicast algorithm. It is based upon rumor routing described in [3].

3.6. Combating Traffic Analysis Attacks

Deng *et al.* propose using a random walk forwarding technique that occasionally forwards a packet to a node other than the sensor's parent node [5].

3.7. Defending against Attacks on Sensor Privacy

There are several techniques to counter many of the attacks levied against a sensor: anonymity mechanisms, policy-based approaches and information flooding.

Anonymity mechanisms depersonalize the data before the data is released, which present an alternative to privacy policy-based access control.

In [9], three main approaches are proposed:

• Decentralize Sensitive Data

• Secure Communication Channel

• Change Data Traffic

• Node Mobility

The access control decisions and authentication are made based on the specifications of the privacy policies. Snekkenes presents advanced concepts for specifying policies in the context of a mobile phone network [22]. Myles and colleagues describe architecture for a centralized location server that controls access from client applications through a set of validator modules that check XML-encoded application privacy policies [14]. In [10] points out that access control decisions can be governed by either room or user policies.

Based on flooding-based routing protocols, Ozturk *et al.* have developed comparable methods for single path routing to try to solve the privacy problems in sensor network. They include Baseline Flooding, Probabilistic Flooding, Flooding with Fake Messages and Phantom Flooding [25].

• **Baseline Flooding** In the baseline implementation of flooding, every node in the network only forwards a message once, and no node retransmits a message that it has previously transmitted. When a message reaches an intermediate node, the node first checks whether it has received and forwarded that message before. If this is its first time, the node will broadcast the message to all its neighbors. Otherwise, it just discards the message.

• **Probabilistic Flooding** In probabilistic flooding, only a subset of nodes within the entire network participate in data forwarding, while others simply discard messages they receive.

• **Flooding with Fake Messages** The previous flooding strategies can only decrease the chances of a privacy violation. An adversary still has a chance to monitor the general traffic and even the individual packets. This observation suggests that one approach to alleviate the risk of source-location privacy breaching is to augment the flooding protocols to introduce more sources that inject fake messages into the network. By doing so, even if the attacker captures the packets, he will have no idea whether the packets are real.

• **Phantom Flooding** Phantom flooding shares the same insights as probabilistic flooding in that they both attempt to direct messages to different locations of the network so that the adversary cannot receive a steady stream of messages to track the source. In phantom flooding, every message experiences two phases: (1) a walking phase, which may be a random walk or a directed walk, and (2) a subsequent flooding meant to deliver the message to the sink. When the source sends out a message, the message is unicast in a random fashion within the first *hwalk* hops. After the *hwalk* hops, the message is flooded using the baseline flooding technique.

3.8. Intrusion Detection

Intrusion detection has focused on two major categories: anomaly based intrusion detection (AID), and misuse intrusion detection (MID) [20]. Anomaly based intrusion detection relies on the assumption that intruders will demonstrate abnormal behavior relative to the legitimate nodes. Thus, the object of anomaly based detection is to detect intrusion based on unusual system behavior. In systems based on misuse intrusion detection, the system maintains a database of intrusion signatures. Using these signatures, the system can easily detect intrusions on the network.

[4] Classifies intrusion detection systems (IDS) into two categories: *host-based* and *network-based*. It describes a series of attacks against several aspects of a wireless sensor network and also introduces three architectures for intrusion detection in wireless sensor networks. The first is termed the stand-alone architecture. Each node functions as an independent intrusion detection system and is responsible for detecting attacks directed toward itself. Nodes do not cooperate in any way. The second architecture is the distributed and cooperative architecture. An intrusion detection agent still resides on each node and nodes are still responsible for detecting attacks against themselves (local attacks), but also cooperate to share information in order to detect global intrusion attempts. The third technique is called the hierarchical architecture. A multi-layered network as one in which the network is divided into clusters with cluster-head nodes responsible for routing within the cluster.

3.9. Secure Data Aggregation

An aggregator is responsible for collecting the raw data from a subset of nodes and processing or aggregating the raw data from the nodes into more usable data. Secure data aggregation techniques will be necessary in many wireless sensor networks.

Przydatek *et al.* focus their efforts on defending specifically against a type of attack called the stealthy attack. In a stealthy attack, the attacker seeks to provide incorrect aggregation results to the user without the user knowing that the results are incorrect. Therefore, the goal of is to ensure that if a user accepts an aggregate value as correct, then there is a high probability that the value is close to the true aggregation value [19].

3.10. Defending against Physical Attacks

Sensor nodes may be equipped with physical hardware to enhance protection against various attacks.

Andersen *et al.* give examples of low-cost protection countermeasures that make such attacks considerably more difficult, including [1]:

• **Randomized Clock Signal** Inserting random-time delays between any observable reaction and critical operations that might be subject to an attack.

• **Randomized Multithreading** Designing a multithread processor architecture that schedules the processor by hardware between two or more threads of execution randomly at a per-instruction level

• **Robust Low-frequency Sensor** Building an intrinsic self-test into the detector. Any attempt to tamper with the sensor should result in the malfunction of the entire processor.

• **Destruction of Test Circuitry** Destroying or disabling the special test circuitry which is for the test engineers, closing the door to microprobing attackers.

• **Restricted Program Counter** Avoid providing a program counter that can run over the entire address space.

• **Top-layer Sensor Meshes** introducing additional metal layers that form a sensor mesh above the actual circuit and that do not carry any critical signals to be effective annoyances to microprobing attackers. For the deployment of components outside the sensor, various approaches have been proposed to protect the sensor, and are summarized in [6].

3.11. Trust Management

Trust can solve some problems beyond the power of the traditional cryptographic security. Zhu *et al.* provide a practical approach to compute trust in wireless networks by viewing individual mobile devices as a node of a delegation graph *G.* An undirected transitive signature scheme is used within the authenticated transitive graphs [28]. In [27], a trust evaluation based security solution is proposed to provide effective security decisions on data protection, secure routing, and other network activities.

4. Conclusion

The paper presented a concise survey on sensor network constraints, security requirements, attacks and defensive measures. As noted, security requirements are critical to preventing an adversary from compromising the security of a distributed wireless sensor network. The key establishment protocols and approaches for distributed wireless sensor networks must satisfy several security and functional requirements.

Further concerns on security of wireless sensor networks exist that are critical but have been left out in this paper for brevity:

- Key cryptography
- Public key based key management
- Privacy and trust
- Data freshness

REFERENCES

[1] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In *IWSP: International Workshop on Security Protocols, LNCS*, 1997.

[2] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. In *Revised Papers from the 8th International Workshop on Security Protocols*, pages 170–177. Springer-Verlag, 2001.

[3] D. Braginsky and D. Estrin. Rumor routing algorthim for sensor networks. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 22–31, New York, NY, USA, 2002. ACM Press.

[4] P. Brutch and C. Ko. Challenges in intrusion detection for wireless ad-hoc networks. In *2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*, 2003.

[5] J. Deng, R. Han, and S. Mishra. Countermeasuers against traffic analysis in wireless sensor networks. Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.

[6] J. Deng, R. Han, and S. Mishra. *Security, privacy, and fault tolerance in wireless sensor networks*. Artech House, August 2005.

[7] J. Douceur. The Sybil attack. In *Proc. of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02)*, February 2002.

[8] S. Ganeriwal, S. ¢Capkun, C.-C. Han, and M. B. Srivastava. Secure time synchronization service for sensor networks. In *WiSe '05: Proceedings of the 4th ACM workshop on Wireless security*, pages 97–106, [30]New York, NY, USA, 2005. ACM Press.

[9] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald. Privacy-aware location sensor networks. In *9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX)*, 2003.

[10] U. Hengartner and P. Steenkiste. Protecting Access to People Location Information. In *Proceedings of First International Conference on Security in Pervasive Computing (to appear)*, LNCS. Springer, Mar 2003.

[11] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang. Fast authenticated key establishment protocols for self-organizing sensor networks. In *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, pages 141–150. ACM Press, 2003.

[12] L. Lazos and R. Poovendran. Secure broadcast in energy-aware wireless sensor networks. In *IEEE International Symposium on Advances in Wireless Communications (ISWC'02)*, 2002.

[13] L. Lazos and R. Poovendran. Serloc: Robust localization for wireless sensor networks. *ACM Trans. Sen. Netw.*, 1(1):73–100, 2005.

[14] G. Myles, A. Friday, and N. Davies. Preserving Privacy in Environments with Location-Based Applications. *IEEE Pervasive Computing*, 2(1):56–64, 2003.

[15] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the third international symposium on Information processing in sensor networks*, pages 259–268. ACM Press, 2004.

[16] P. Papadimitriou and Z. J. Haas. Secure routing for mobile ad hoc networks. In *Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference (CNDS 2002)*, 2002.

[17] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *Proceedings of IEEE Symposium on Security and Privacy*, May 2005.

[18] R. Di Pietro, L. V. Mancini, Y. W. Law, S. Etalle, and P. Havinga. LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. In *First International Workshop on Wireless Security and Privacy (WiSPr'03)*, 2003.

[19] B. Przydatek, D. Song, and A. Perrig. Sia: Secure information aggregation in sensor networks, 2003.

[20] I. Sato, Y. Okazaki, and S. Goto. An improved intrusion detection method based on process profiling. *IPSJ Journal*, 43(11):3316–3326, 2002.

[21] B. Schneier. *Applied Cryptography*. Second Edition, John Wiley & Sons, 1996.

[22] E. Snekkenes. Concepts for personal location privacy policies. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 48–57. ACM Press, 2001.

[23] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy. Poster abstract secure locations: routing on trust and isolating compromised sensors in location aware sensor networks. In *Proceedings of the 1st international conference on embedded networked sensor systems*, pages 324–325. ACM Press, 2003.

[24] S. ¢Capkun and J.-P. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, 2006.

[25] X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii. Search-based physical attacks in sensor networks: Modeling and defense. Technical report, Dept. of Computer Science and Engineering, The Ohio-State University, February 2005.

[26] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. *Computer*, 35(10):54–62, 2002.

[27] Z. Yan, P. Zhang, and T. Virtanen. Trust evaluation based security solution in ad hoc networks. In *NordSec 2003, Proceedings of the Seventh Nordic Workshop on Secure IT Systems*, 2003.

[28] H. Zhu, F. Bao, R. H. Deng, and K. Kim. Computing of trust in wireless networks. In *Proceedings of 60th IEEE Vehicular Technology Conference*, Los Angles, California, September 2004.

[29] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for largescale distributed sensor networks. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 62–72, New York, NY, USA, 2003. ACM Press.

[30] http://www.zigbee.org/, 2005.