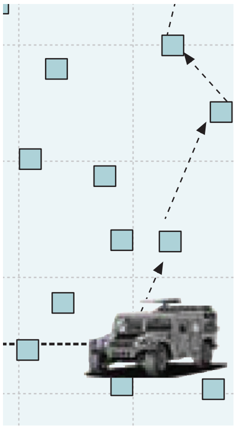
SECURITY IN WIRELESS SENSOR NETWORKS

XIAOJIANG DU, NORTH DAKOTA STATE UNIVERSITY
HSIAO-HWA CHEN, NATIONAL CHENG KUNG UNIVERSITY



Sensor networks hold the promise of facilitating large-scale and real-time data processing in complex environments. Security is critical for many sensor network applications, such as military target tracking and security monitoring.

ABSTRACT

Recent advances in electronics and wireless communication technologies have enabled the development of large-scale wireless sensor networks that consist of many low-power, low-cost, and small-size sensor nodes. Sensor networks hold the promise of facilitating large-scale and real-time data processing in complex environments. Security is critical for many sensor network applications, such as military target tracking and security monitoring. To provide security and privacy to small sensor nodes is challenging, due to the limited capabilities of sensor nodes in terms of computation, communication, memory/storage, and energy supply. In this article we survey the state of the art in research on sensor network security.

INTRODUCTION

Wireless sensor networks have applications in many important areas, such as the military, homeland security, health care, the environment, agriculture, and manufacturing. One can envision in the future the deployment of large-scale sensor networks where hundreds and thousands of small sensor nodes form self-organizing wireless networks. Providing security in sensor networks is not an easy task. Compared to conventional desktop computers, severe constraints exist since sensor nodes have limited processing capability, storage, and energy, and wireless links have limited bandwidth. Despite the aforementioned challenges, security is important and even critical for many applications of sensor networks, such as military and homeland security applications. Several recent contributions to the literature have addressed security and privacy issues in sensor networks [1–11]. In this article we discuss current and past research activities carried out on sensor network security.

The rest of the article is outlined as follows. We summarize typical attacks on sensor networks. We give typical assumptions and security objectives of sensor networks. Then we discuss key management, secure time synchronization, secure location discovery, and secure routing, respectively. Finally, we conclude this article. Due to page limits, we do not extensively discuss other sensor network security issues, such as broadcast authentication and detection of compromised sensor nodes.

ATTACKS ON WIRELESS SENSOR NETWORKS

A large-scale sensor network consists of thousands of sensor nodes and may be dispersed over a wide area. Typical sensor nodes are small with limited communication and computing capabilities, and are powered by batteries. These small sensor nodes are susceptible to many kinds of attacks. For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Attacks on sensor networks can be classified into attacks on physical, link (medium access control), network, transportation, and application layers. Attacks can also be classified based on the capability of the attacker, such as sensor-level and laptop-level. A powerful laptop-level adversary can do much more harm to a network than a malicious sensor node, since it has much better power supply, as well as larger computation and communication capabilities than a sensor node. Attacks can also be classified into outside and inside attacks. An outside attacker has no access to most cryptographic materials in sensor networks, while an inside attacker may have partial key materials and the trust of other sensor nodes. Inside attacks are much harder to detect and defend against. In [1] Wood and Stankovic classified various denial of sservice (DoS) attacks on sensor networks according to network layers. The attacks include DoS attacks as studied in [1] and attacks identified in other literature, such as [2, 3]. For each type of attack, three items are presented in the following order: the name of the attack, the corresponding network layer, and possible defense techniques. We summarize typical attacks on sensor networks and possible defense techniques below:

1 Jamming (physical layer): spread-spectrum, lower duty cycle
2 Tampering (physical layer): tamper-proofing, effective key management schemes
3 Collision (link layer): error correcting code
4 Exhaustion (link layer): rate limitation
5 Manipulating routing information (network layer): authentication, encryption
6 Selective forwarding attack (network layer): redundancy, probing
7 Sybil attack (network layer): authentication

1536-1284/08/$25.00 © 2008 IEEE

8 Sinkhole (blackhole) attack (network layer): authentication, monitoring, redundancy
9 Wormhole attack (network layer): monitoring, flexible route selection
10 Hello flood attack (network layer): two-way authentication, three-way handshake
11 Flooding (transport layer): limiting connection numbers, client puzzles
12 Clone attack (application layer): unique pairwise keys

Because of the page limit, we do not explicitly explain these attacks. Details can be found in [1–3].

Security Objectives for Sensor Networks

Wireless sensor networks have many unique features that differ from mobile ad hoc networks and other wireless (and wired) networks. When considering security in sensor networks, we need to give assumptions on the network. Some typical assumptions made in the existing literature are listed below.

Typical Assumptions

Since sensor nodes use wireless communications, radio links are generally insecure. Eavesdropping, injection, replay, and other attacks can be placed on the network. The adversary is able to deploy malicious nodes in the network, or compromises some legitimate nodes. Most papers published in the literature on sensor network security do not assume that sensor nodes are tamper resistant since the corresponding investment adds significant per-unit cost to sensor nodes. A typical assumption is to assume that base stations are well protected and trusted. Since a base station is the gateway for sensor nodes to communicate with the outside world, compromising the base station could render the entire sensor network useless. Thus, base stations in sensor networks are assumed to be secure.

Other typical assumptions on sensor networks are:

- Sensor nodes are densely and statically deployed in the network.
- Sensor nodes are aware of their own locations.

Location awareness is a basic requirement for sensor nodes in many sensor networks, since most sensing data must be associated with the locations where data is generated. The network may use localization services to estimate the locations of individual nodes, and no GPS receiver is required at each sensor. There are other particular assumptions made in some work that may limit the applicability of the proposed schemes.

Security Objectives

The ultimate security objective is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. Every eligible receiver should receive all messages intended for it and be able to verify the integrity of every message as well as the identity of the sender. Adversaries should not be able to infer the contents of any message. In conventional computer networks the primary security goal is reliable delivery of messages (i.e., protection against DoS attack). Message authenticity, integrity, and confidentiality are usually achieved by an end-to-end security mechanism such as Secure Socket Layer (SSL). The reason is because the dominating traffic pattern is end-to-end communication, where it is neither necessary nor desirable for the contents of the message (beyond the necessary headers) to be available to the intermediate routers. However, the dominant traffic pattern in sensor networks is many-to-one, as illustrated in Fig. 1, where a large number of sensor nodes sending data to one (or a few) base station(s) at the top right corner. In-network processing such as data aggregation, duplicate elimination, or data compression is very important for sensor networks to run in an energy-efficient manner. For example, sensor node D in Fig. 1 receives data from three sensors that detect the same event. Data aggregation at node D can significantly reduce communication cost. Since in-network processing requires intermediate nodes to access, modify, and possibly suppress the contents of messages, it is highly unlikely that end-to-end security mechanisms between a sensor node and a base station can be used to guarantee integrity, authenticity, and confidentiality of such messages.

In the presence of insider adversaries, link layer security is not enough to protect the whole network, since an insider has complete access to any message routed through it, and it can modify, suppress, or even discard the message. In such a case one might not be able to provide confidentiality, integrity, authenticity, and avail-

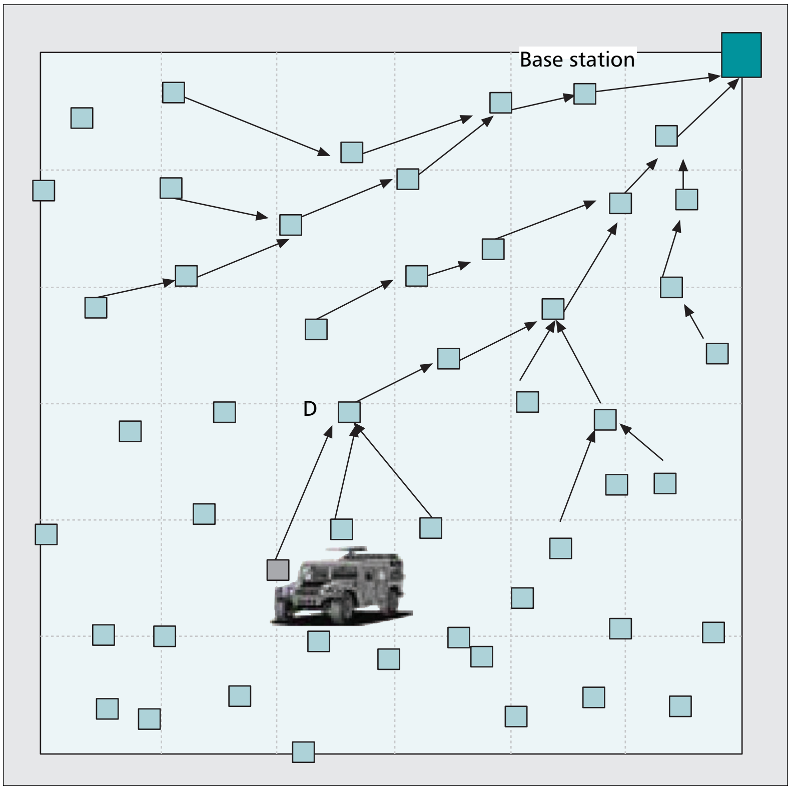


Figure 1. *The many-to-one traffic pattern and in-network processing in sensor networks.*

To achieve security in wireless sensor networks, it is important to be able to perform various cryptographic operations. Keys for these cryptographic operations must be set up by communicating nodes before they can exchange information securely.

ability to every message. Thus, in the presence of insider attacks, the security objectives should be to ensure that the sensor network can provide the basic functionalities (i.e., performing sensing and transmitting data to the base station) with minimum degradation. In the next section we discuss a number of important security issues in sensor networks, including key management, secure time synchronization, secure location discovery, and secure routing.

Key Management

To achieve security in wireless sensor networks, it is important to be able to perform various cryptographic operations, including encryption, authentication, and so on. Keys for these cryptographic operations must be set up by communicating nodes before they can exchange information securely. Key management schemes are mechanisms used to establish and distribute various kinds of cryptographic keys in the network, such as individual keys, pairwise keys, and group keys. Key management is an essential cryptographic primitive upon which other security primitives are built. Most security requirements, such as privacy, authenticity, and integrity, can be addressed by building on a solid key management framework. In fact, a secure key management scheme is the prerequisite for the security of these primitives, and thus essential to achieving secure infrastructure in sensor networks. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial.

The challenge of designing key management protocols for sensor networks lies in establishing a secure communication infrastructure, before any routing fabric has been established with or without the presence of any trusted authority or fixed server, from a collection of sensor nodes that have no prior contact with each other. Some cryptographic information (e.g., a key) is normally preloaded in sensor nodes before deployment, and allows sensor nodes to perform secure communications with each other. Most schemes do not assume prior knowledge of the network deployment topology and allow nodes to be added to the network after deployment. The schemes must have low computational and low storage requirements. There are four types of key management schemes: trusted server, self-enforcing, key predistribution, and public key cryptography. We discuss these schemes in the following subsections.

Trusted Server Schemes

Trusted server schemes depend on a trusted and secure server such as the base station for key agreement among nodes. The server can be treated as the key distribution center (KDC). For example, assume that two sensor nodes intend to make a secure connection. In a typical case, a symmetric key is generated for each node in a sensor network before deployment and embedded in each sensor node's memory. This embedded key is used for the two sensors to authenticate themselves to the base station. Then the base station generates a link key or session key and sends it securely to both sensor nodes via a single hop or multiple hops. In the trusted server scheme the base station is the most appropriate choice for the server, and each sensor node stores only an embedded key such that a compromising/captured node cannot reveal much security information of the sensor network. The drawback of the trusted server scheme is that if the server is compromised, the network is totally unsecured. However, we usually assume that the base station where the server runs is secured.

Self-Enforcing Schemes

A self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates. If the sensor node can support the computationally intensive asymmetric cryptographic operations, key distribution via asymmetric cryptography is a favored scheme (e.g., the schemes proposed in [9, 10]). Sensor nodes conduct exchanges of public keys and master key signatures after deployment. A sensor node is legitimate if the master key's signature is verified using the master public key. A symmetric session key for a sensor node can be generated and sent using the sensor node's public key. In a self-enforcing scheme, a compromising sensor node reveals no security information about other keys in the network except current ongoing session keys. However, limited computation and energy resources of sensor nodes make it undesirable to use public key algorithms such as Diffie-Hellman key agreement or RSA.

Key Predistribution Schemes

The third type of key agreement scheme is key predistribution, where key information is distributed among all sensor nodes prior to deployment. Recent research on sensor networks suggests that key predistribution schemes are a promising practical option for scenarios where the network topology is not known prior to deployment. Eschenauer and Gligor [4] first presented a key management scheme for sensor networks based on probabilistic key predistribution. Chan *et al.* [5] extended this scheme and presented three mechanisms for key establishment. Liu and Ning [6] proposed a key management scheme based on key predistribution to establish pairwise keys in sensor networks. In [7] Perrig *et al.* proposed SPINS, a suite of security building blocks for sensor networks. SPINS includes SNEP, a protocol for data confidentiality and two-party data authentication, and mTESLA, a protocol for broadcast data authentication.

Public-Key-Cryptography-Based Schemes

Public key cryptography has been considered too expensive for small sensor nodes, because typical public key algorithms (e.g., RSA) require extensive computations and are not suitable for tiny sensors. The recent implementation of 160-bit elliptic curve cryptography (ECC) on Atmel ATmega128, a CPU of 8 MHz and 8 bits, demonstrates that ECC public key cryptography is feasible for sensor nodes [8]. Compared to symmetric key cryptography, public key cryptography provides a more flexible and simpler interface, requiring no key predistribution, no pair-wise key sharing, and no complicated one-way keychain scheme. Several works (e.g., [8–10]) discuss ways to utilize public key cryptography to provide security for sensor networks. Malan *et al.* [9] implemented ECC in 8-bit 7.3828-MHz MICA2 mote sensors, and their experiments showed that public keys can be generated within 34 s, and the storage used is about 1 kbyte of SRAM and 34 kbytes of ROM. Wander *et al.* [10] measured the energy consumption of authentication and key exchange based on public key cryptography on an 8-bit CPU, and compared two public key algorithms, RSA and ECC. In [10] the authors also showed that energy consumption of communication forms a larger fraction of the overall energy than that of security operations. The same group [8] also demonstrated that ECC consumes significantly less energy, execution time, and memory than does RSA. For example, an ECC-160 (key length is 160 bits) point multiplication takes only 1.61 s and 282 bytes of data memory, while an RSA-1024 (key length is 1024 bits) private key modular exponentiation takes nearly 22 s and 930 bytes of data memory.

SECURE TIME SYNCHRONIZATION

Due to the collaborative nature of sensor nodes, time synchronization is very important for many sensor network operations, such as coordinated sensing tasks, sensor scheduling (sleep and wake), mobile object tracking, time-division multiple access (TDMA) medium access control, data aggregation, and multicast source authentication protocol. For example, in the target tracking application illustrated in Fig. 2, sensor nodes need to know both the location where and time when the target is sensed in order to correctly determine the target moving direction and speed.

The Network Time Protocol (NTP) [11] is used for synchronization in the Internet. A sensor network is a resource constrained distributed system, and the NTP cannot be directly used by sensor networks. Several time synchronization algorithms (e.g., [12, 13]) have been proposed for sensor networks. All network time synchronization methods rely on some kind of message exchanges between nodes. Nondeterminism in the network dynamics, such as physical channel access time and operation system overhead (e.g., system calls), makes synchronization implementation challenging in sensor networks. The proposed time synchronization schemes for sensor networks include Reference-Broadcast Synchronization (RBS) [12], Timing-Sync Protocol for Sensor Networks (TPSN) [13], and so on. These time synchronization algorithms try to achieve either pair-wise clock synchronization or global clock synchronization. Pair-wise clock synchronization aims to obtain high-precision clock synchronization between pairs of sensor neighbors, while global clock synchronization aims to provide network-wide clock synchronization in the whole sensor network.

Existing pair-wise clock synchronization protocols use either receiver–receiver synchronization (e.g., RBS [12]), in which a reference node broadcasts a reference packet to help pairs of receivers identify the clock differences, or sender–receiver synchronization (e.g., TPSN [13]), where a sender communicates with a receiver to estimate the clock difference. Most of the global clock synchronization protocols establish multihop paths in a sensor network so that all nodes can synchronize their clocks to a given source based on these paths and the pair-wise clock differences between adjacent nodes in these paths.

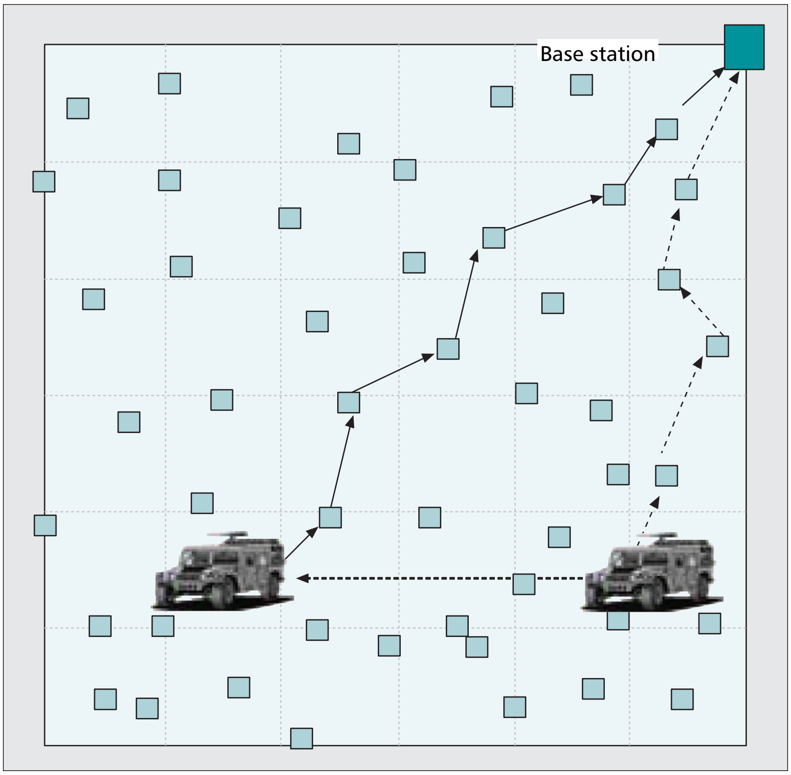


Figure 2. *Target tracking in a sensor network.*

However, none of the aforementioned time synchronization schemes were designed with security in mind. Hence, they are not suitable for applications in hostile environments (e.g., military battlefields) where security is critical. Most existing time synchronization schemes are vulnerable to several attacks. In [14] the authors identified four possible attacks on sensor time synchronization:

- Masquerade attack: Suppose that node A sends out a reference beacon to its two neighbors, B and C. An attacker, E, can pretend to be B and exchange wrong time information with C, disrupting the time synchronization process between B and C.
- Replay attack: Using the same scenario as mentioned in the first attack, attacker E can replay B's old timing packets, misleading C to be synchronized to a wrong time.
- Message manipulation attack: In this attack, an attacker may drop, modify, or even forge the exchanged timing messages to interrupt the time synchronization process.
- Delay attack: The attacker deliberately delays some of the time messages (e.g., the beacon message in the RBS scheme) so as to fail the time synchronization process. It is noted that this attack cannot be defended against by cryptographic techniques.

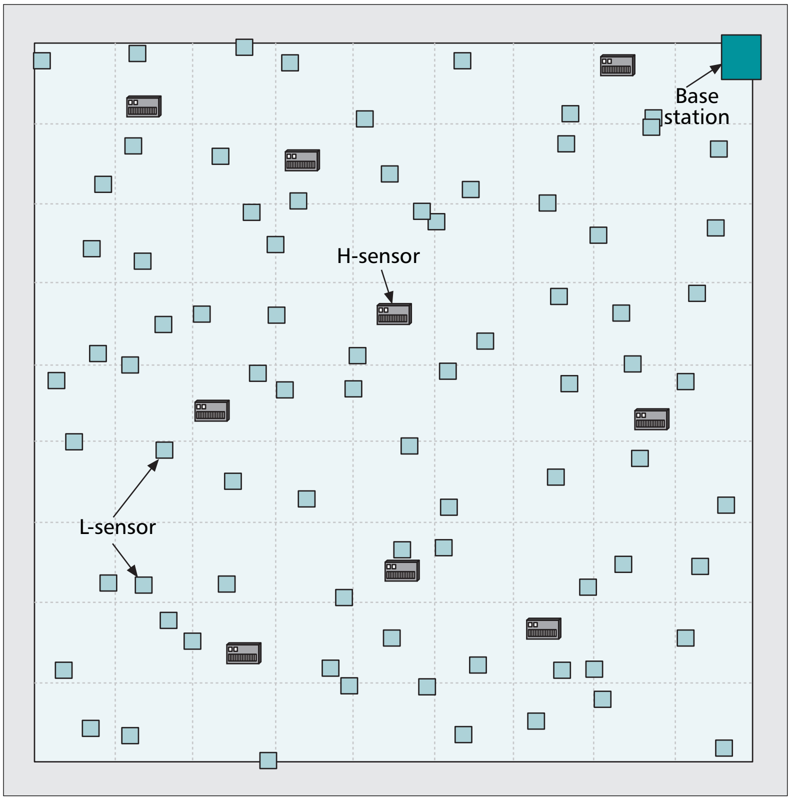


Figure 3. *An heterogeneous sensor network.*

In addition to the above four attacks, denial-of-service (DoS) attack can also disrupt most time synchronization schemes. For example, an adversary can cause jamming or packet collision with timing messages, and thus disrupt the time synchronization process. The first three attacks can be addressed by cryptographic techniques. Authentication can be used to defend against a masquerade attack. For example, a sensor network can first use a key management scheme to establish shared keys for each pair of neighbor sensors. Then a sender can calculate a message authentication code (MAC) by using the shared key and append the MAC to an outgoing message. The MAC prevents an attacker from impersonating other nodes or altering the message content without being detected. To prevent a replay attack, a sequence number can be added to each exchanged message. Message dropping may be noticed by some misbehavior detection schemes. However, delay and DoS attacks cannot be defended against by cryptographic techniques.

In [14] Song *et al.* identified the delay attack and propose solutions to defend against it. The general idea in [14] is to collect a set of time offsets from multiple involved nodes, and some statistical methods are used to identify the malicious time offsets (from attackers). Then the identified malicious time offsets are excluded, and the rest of the time offsets are used to estimate the actual time offsets. Two schemes were proposed in [14] to defend against the delay attack. The first scheme uses a statistical method, or the generalized extreme studentized deviate (GESD) algorithm, to detect multiple outliers introduced by the compromised nodes, and the second scheme utilizes a threshold derived using a time transformation technique to filter out the outliers.

In [1] Wood and Stankovic discussed DoS attacks in sensor networks and listed possible defense schemes against these attacks. For example, spread-spectrum technique may be used to avoid jamming attack, and error-correcting code may be used to defend packet collision attack. In general, it is not an easy task to detect and defend DoS attacks in sensor networks.

The above time synchronization schemes are designed for homogeneous sensor networks, where all sensor nodes are modeled to have the same capabilities. These schemes involve nontrivial computation and communications, and thus incur large overhead. Furthermore, many synchronization algorithms need to propagate a time synchronization message from some reference point (e.g., the base station) to all sensors via multiple hops, and synchronization error can be accumulated during the multihop transmissions.

In [15] Du *et al.* proposed a secure, efficient, and effective time synchronization scheme for heterogeneous sensor networks, which include physically different types of sensor nodes. The scheme achieves stronger security and better efficiency by utilizing the long transmission range and other features of high-end sensors. Figure 3 shows a heterogeneous sensor network, where the small squares represent low-end sensors, large rectangular nodes are high-end sensors, and the large square at the top right corner is the base station. For example, MICA2-DOT sensors (as shown in the top left corner of Fig. 4) may function as low-end sensors, and Stargate nodes (as shown at the bottom of Fig. 4) may serve as high-end sensors. Both sensor nodes are manufactured by Crossbow Technology Inc. In the top right of Fig. 4 is a quarter used to show the sensor's size.

SECURE LOCATION DISCOVERY

As mentioned earlier, sensor locations play a critical role in many sensor network applications, such as environment monitoring and target tracking. Furthermore, several fundamental techniques developed for wireless sensor networks also require sensor location information, such as geographical routing protocols that make routing decisions based on node locations. Indeed, many sensor network applications will not work without sensor location information. Many location discovery/estimation (also called localization) protocols have been proposed for sensor networks, for instance, the scheme suggested in [16]. These protocols share a common feature: they all should make use of some special nodes, called beacon nodes, which are assumed to know their own locations (e.g., through GPS receivers or manual configuration). These protocols work in two stages. In the first stage nonbeacon nodes receive radio signals called reference messages from the beacon nodes. A reference message includes the location of the beacon node. In the second stage the nonbeacon nodes then make certain measurements (e.g., distance between the beacon and nonbeacon nodes) based on features of the reference messages (e.g., received signal strength indicator [RSSI], time difference of arrival). Without protection, an attacker may easily mislead the location estimation at sensor nodes and subvert the normal operation of sensor networks. For example, an attacker may provide incorrect location references by replaying the beacon packets intercepted in different locations. Moreover, an attacker may compromise a beacon node and distribute malicious location references by lying about the location or manipulating the beacon signals (e.g., changing the signal strength if RSSI is used to estimate the distance). In either case, nonbeacon nodes will determine their locations incorrectly. Recently, several secure/robust localization schemes have been proposed. In [17] the authors proposed two approaches to dealing with malicious attacks against location discovery in wireless sensor networks. The first approach is based on minimum mean square estimation (MMSE). The mean square error is used as an indicator to identify and remove malicious location references. The second approach uses a voting-based location estimation technique and iteratively refines voting to tolerate malicious location references sent by attackers. In [18] Du *et al.* formulated a secure localization problem as an anomaly intrusion detection issue and proposed a few schemes to detect localization anomalies caused by attackers.

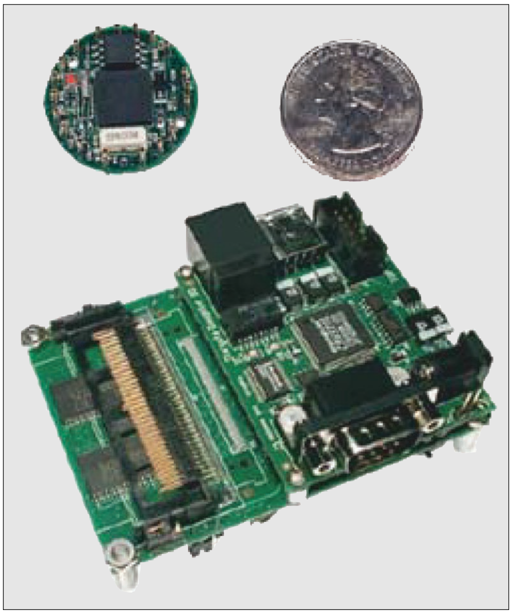


Figure 4. *Heterogeneous sensor nodes.*

Security is critical for many sensor networks. Many security issues in wireless sensor networks remain open and we expect to see more research activities on these exciting topics in the future.

Secure Routing

The primary functionality of wireless sensor networks is to sense the environment and transmit the acquired information to base stations for further processing. Thus, routing is an essential operation in sensor networks. A number of routing protocols have been proposed for sensor networks. However, previous research on sensor network routing was focused very much on efficiency and effectiveness of data dissemination, and very few studies considered security issues in the design of the routing protocol. Studies and experiences (e.g., [2]) have shown that considering security in the design stage is the best way to provide security for sensor network routing. Several secure routing protocols have been proposed for mobile ad hoc networks (MANETs). However, these protocols are not suitable for sensor networks because:

- They require lots of computations for routing and security.
- They were designed to find and establish routes between any pair of nodes, which is different from the many-to-one traffic pattern dominant in sensor networks.

In [1] Wood and Stankovic identified a number of DoS attacks in sensor networks. Many of these DoS attacks are on sensor network routing. In [2] Karlof and Wagner described several security attacks on routing protocols in sensor networks. They also analyzed the possible attacks on several existing routing protocols, including Directed Diffusion and LEACH. However, Karlof and Wagner did not present any secure routing protocol for sensor networks in [2]. In [19] Du *et al.* proposed an efficient and secure routing protocol for heterogeneous sensor networks. The protocol achieves energy efficiency and can defend against many typical attacks on sensor routing. In [20] Ye *et al.* considered how to efficiently detect false data injected by compromised nodes.

Conclusions

Security is critical for many sensor networks. Due to the limited capabilities of sensor nodes, providing security and privacy to a sensor network is a challenging task. In this article, we summarize typical attacks on sensor networks and surveyed the literatures on several important security issues relevant to the sensor networks, including key management, secure time synchronization, secure location discovery, and secure routing. Many security issues in wireless sensor networks remain open and we expect to see more research activities on these exciting topics in the future.

References

[1] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," *Computer*, vol. 35, no. 10, Oct. 2002, pp. 54–62.

[2] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *Proc. 1st IEEE Int'l. Wksp. Sensor Network Protocols and Apps.*, 2003.

[3] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," *Computer*, vol. 36, no. 10, Oct. 2003, pp. 103–05.

[4] L. Eschenauer and V. D. Gligor. "A Key Management Scheme for Distributed Sensor Networks," *Proc. 9th ACM Conf. Comp. and Commun. Sec.*, Nov. 2002, pp. 41–47.

[5] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *Proc. 2003 IEEE Symp. Sec. and Privacy*, May 2003, pp. 197–213.

[6] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *Proc. 10th ACM Conf. Comp. and Commun. Sec.*, 2003, pp. 52–61.

[7] A. Perrig *et al.*, "SPINS: Security Protocols for Sensor Networks," *Proc. 7th ACM MOBICOM*, 2001.

[8] N. Gura *et al.*, "Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs," *Proc. 6th Int'l. Wksp. Cryptographic Hardware and Embedded Sys.*, Boston, MA, Aug. 2004.

[9] D. Malan, M. Welsh, and M. D. Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography," *Proc. 1st IEEE Int'l. Conf. Commun. and Networks*, Santa Clara, CA, Oct. 2004.

[10] A. S. Wander *et al.*, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," *Proc. 3rd IEEE Int'l. Conf. Pervasive Computing and Commun.*, 2005.

[11] D. L. Mills, Taylor, and Francis, *Computer Network Time Synchronization: The Network Time Protocol*, CRC Press.

[12] M. L. Sichitiu and C. Veerarittiphan, "Simple, Accurate Time Synchronization for Wireless Sensor Networks," *Proc. WCNC 2003*.

[13] S. Ganeriwal, R. Kumar, and M. B. Srivastava, "Timing-Sync Protocol for Sensor Networks," *Proc. 1st Int'l. Conf. Embedded Networked Sensor Sys.*, 2003, pp. 138–49.

[14] H. Song, S. Zhu, and G. Cao, "Attack-Resilient Time Synchronization for Wireless Sensor Networks," *Proc. 2nd IEEE Int'l. Conf. Mobile Ad Hoc and Sensor Sys.*, Washington, DC, Nov. 2005.

[15] X. Du *et al.*, "Secure and Efficient Time Synchronization in Heterogeneous Sensor Networks," *IEEE Trans. Vehic. Tech.*, vol. 57, no. 4, July 2008, pp. 2387–94.

[16] T. He *et al.*, "Range-Free Localization Schemes in Large Scale Sensor Networks," *Proc. ACM MobiCom 2003*, 2003.

[17] D. Liu, P. Ning, and W. Du, "Attack-Resistant Location Estimation in Sensor Networks," *Proc. 4th Int'l. Symp. Info. Processing in Sensor Networks*, pp. 99–106, Apr. 2005.

[18] W. Du, L. Fang, and P. Ning, "LAD: Localization Anomaly Detection for Wireless Sensor Networks," *J. Parallel and Distrib. Comp.*, vol. 66, no. 7, July 2006, pp. 874–86.

[19] X. Du *et al.*, "Two Tier Secure Routing Protocol for Heterogeneous Sensor Networks," to appear, *IEEE Trans. Wireless Commun.*

[20] F. Ye *et al.*, "Statistical En-route Detection and Filtering of Injected False Data in Sensor Networks," *Proc. IEEE INFOCOM '04*.

BIOGRAPHIES

XIAOJIANG (JAMES) DU (dxj@ieee.org) is an assistant professor in the Department of Computer Science at North Dakota State University. He received his B.E. degree from Tsinghua University, Beijing, China, in 1996, and his M.S. and Ph.D. degrees from University of Maryland, College Park in 2002 and 2003, respectively, all in electrical engineering. His research interests are heterogeneous wireless sensor networks, security, wireless networks, computer networks, network and systems management, and controls. He has published over 50 journal and conference papers in the above areas. His research is supported by the National Science Foundation (NSF), Army Research Office, and National Aeronautics and Space Administration (NASA). He is an Associate Editor of four international journals: *Wireless Communication and Mobile Computing* (Wiley), *Security and Communication Networks* (Wiley), *Journal of Computer Systems, Networking, and Communications* (Hindawi), and *International Journal of Sensor Networks* (Inder-Science). He is (was) the Chair of Computer and Network Security Symposium of the ACM International Wireless Communication and Mobile Computing Conference 2008, 2007, and 2006. He is (was) a Technical Program Committee member of several major IEEE conferences such as INFOCOM, ICC, GLOBECOM, WCNC, IM, NOMS, BroadNet, and IPCCC.

HSIAO-HWA CHEN (hshwchen@ieee.org) is currently a full professor in the Department of Engineering Science, National Cheng Kung University, Taiwan, and was the founding Director of the Institute of Communications Engineering of National Sun Yat-Sen University, Taiwan. He received B.Sc. and M.Sc. degrees from Zhejiang University, China, and a Ph.D. degree from the University of Oulu, Finland, in 1982, 1985, and 1990, respectively, all in electrical engineering. He has authored or co-authored over 200 technical papers in major international journals and conferences, five books, and several book chapters in the areas of communications, including the books *Next Generation Wireless Systems and Networks* and *The Next Generation CDMA Technologies* (Wiley, 2005 and 2007). He has been an active volunteer for various IEEE technical activities for over 20 years. Currently, he is serving as Chair of the IEEE ComSoc Radio Communications Committee and Vice Chair of the IEEE ComSoc Communications & Information Security Technical Committee. He served or is serving as symposium chair/co-chair of many major IEEE conferences, including VTC, ICC, GLOBECOM, and WCNC. He served or is serving as Associate Editor or/and Guest Editor of numerous important technical journals in communications. He is serving as Chief Editor (Asia and Pacific) for Wiley's *Wireless Communications and Mobile Computing Journal* and Wiley's *International Journal of Communication Systems*. He is the founding Editor-in-Chief of Wiley's *Security and Communication Networks* journal (www.interscience.wiley.com/journal/security). He is also an adjunct professor of Zhejiang University, China, and Shanghai Jiao Tong University, China.