17

Security of Wireless Sensor Networks: Current Status and Key Issues

Chun-Ta Li
Department of Information Management, Tainan University of Technology
Taiwan

1. Introduction

Due to significant advances in wireless and mobile communication techniques and the broad development of potential applications, Wireless Sensor Networks (WSNs) have attracted great attention in recent years. Nevertheless, WSNs are formed dynamically by a number of power-limited sensor nodes and the manager node with long-lasting power. WSNs are self-organized and autonomous systems consisting of common sensors, manager nodes and back-end data center. Firstly, the common sensors are responsible for transmitting the real-time sensor data of specific monitoring environment to the intermediate collection nodes called manager node. Finally, the back-end data center will receive the sensed data from manager nodes to do further process and analysis. Undoubtedly, all communication between nodes are through the wireless transmission techniques. Furthermore, due to the property of self-organized, without support from the fixed infrastructure and the topology of wireless sensor network changes dynamically, therefore, broadcasting is the general way for communications in WSNs.
Wireless sensor network has been widely used in practical applications, such as monitoring of forest fire, detection of military purpose, medical or science areas and even in our home life. However, WSNs are easily compromised by attackers due to wireless communications use a broadcast transmission medium and their lack of tamper resistance. Therefore, an attacker can eavesdrop on all traffic, inject malicious packets, replay older messages, or compromise a sensor node. Generally, sensor nodes are most worried about two major security issues, which are privacy preserving and node authentication. Privacy means the data confidentiality is achieved under security mechanism, and hence it allows network communications between sensor nodes and the manager station to proceed securely. In addition, a well-structured authentication mechanism can ensure that no unauthorized node is able to fraudulently participate and get sensitive information from WSNs. As a result, several schemes have been proposed to secure communications in WSNs. In this chapter, we classify them into three classifications based on the cryptographic techniques: symmetric keys, asymmetric keys and one-way hashing functions.
The rest of this chapter is organized as follows: In Section 2, we introduce the characteristics and consideration of WSNs. In Section 3, we review some security threats and requirements in WSNs. Section 4 is for the security countermeasure schemes and its classification. Finally, we conclude some future works for the secure networking in WSNs.

2. Wireless Sensor Network

Compared with the traditional communication networks, some characteristics and considerations for wireless sensor networks are discussed and addressed in the design of WSNs. These are briefly reviewed in this section.

2.1 Characteristics of Wireless Sensor Network

- **Non-centralized architecture**: In WSNs, the status of every node is identical and no one is responsible for providing normal services. It is lack of a central administration and every node can join or disjoin the network any time. Besides, it does not affect the whole sensor network if some node failed and is reliable for applications with high stable requirement.
- **Self-organized**: Because WSNs are characterized as infrastructure-less networks and lack of fixed infrastructure. Thus, the sensor network is fully constructed by themselves when it is begin working with some pre-defined layering protocols and distributed algorithms. Once sensor networks are constructed completely, the sensor data would be collect and send to back-end system for further processing through the networks they built.
- **Multi-hop routing**: The sensor range of nodes in the WSNs is assumed to be limited, so if a node A would like to communicate with node D, which is out of communication range of node A. The node B would be a intermediate node and is responsible for transmitting the communication data to each other between node A and node B. The multi-hops is illustrated as Figure 1.
- **Dynamic topology**: In most of sensor network architecture assume that sensor nodes are deployed randomly and the network topology would be changed dynamically since the sensor node might be shut down, crash, recovery or utilize mobile sensors.

2.2 Consideration of Wireless Sensor Networks

- **Hardware constraints**: This part is related to physical property and many constraints on these areas have been proposed. For example, limited energy. In addition, due to the influence of limited volume of the sensor, some sensor can only provide limited storage, limited bandwidth, limited energy and limited computation ability.
- **Communication**: The existing communicating schemes show that there are three main types of communications in WSNs; including direct, clustering-based, and multi-hops communication. In direct communication, every sensor node transmits its sensor data to a manager node and the manager node is responsible for collecting these data to back-end data center for further processing. In clustering communication, all sensor nodes are divided into several groups and each cluster head node is responsible for collecting data within its group. Multi-hops communication is used because the communication range of a sensor is assumed to be limited and the neighboring sensor nodes maybe used for transmitting the communication packets to each other on their path between the source node and the destination node.
- **Scalability**: Another consideration is the scalability of sensor networks. In this case, networking must keep on working whatever the number of sensor nodes are placed will not be affected.

- **Fault tolerance**: Due to the influence of applied environment on sensors, many exceptions have been addressed in sensor networks. For example, sensors may crash, power failure or shut down etc. Such problems need to be avoided by the strategies of fault tolerance to keep on networking.
- **Power saving**: When the sensors are distributed to monitor some environments of interest, these sensors may work over a long span of several weeks even for months. Therefore, how to provide a mechanism of power saving to extend its lifespan is highly important. In general, there's too great a consumption of power during the transmitting message phase.
- **Cost**: Depending on the application of sensor network, a large number sensors might be scattered randomly over an environment, such as weather monitoring. If the overall cost was appropriate for sensor networks and it will be more acceptable and successful to users which need careful consideration.
- **Mobility**: In clustered (hierarchical) WSNs, sensor nodes are typically organized into many clusters, with cluster controllers collecting sense data from ordinary sensor nodes in the managed cluster to the back-end data center. Furthermore, compared to mobile ad hoc networks, when sensor nodes are randomly deployed in a designated area, they only infrequently move from one cluster to another, and thus mobility is not a critical issue in WSNs.
- **Sleep pattern**: The sleep pattern is highly necessary in WSNs to extend the availability of the networks. For example, the manager node can set fresh bootstrapping times for live sensors while other sensor nodes can shut down to save power. Different sensor nodes are operated according to the bootstrapping times to which they belong and the lifetime of WSNs is therefore extended in a differentiated way (23).
- **Security**: One of the challenges in WSNs is to provide high-security requirements with constrained resources. The security requirements in WSNs are comprised of node authentication, data confidentiality, anti-compromise and resilience against traffic analysis. To identify both trustworthy and unreliable nodes from a security standpoints, the deployment sensors must pass an node authentication examination by their corresponding manager nodes or cluster heads and unauthorized nodes can be isolated from WSNs during the node authentication procedure. Similarly, all the packets transmitted between a sensor and the manager node must be kept secret so that eavesdroppers cannot intercept, modify and analyze, and discover valuable information in WSNs.

3. Security Threats and Requirements in Wireless Sensor Networks

In addition to the characteristics and considerations mentioned above, security threats and requirements are also critical for a variety of sensor network applications. In recent years, there are several security issues in WSNs have been proposed. In this section, we will introduce some security threats and requirements in WSNs.

1. Passive attacks : In passive attacks (such as eavesdropping attacks), eavesdroppers can unintrusively monitor on the communication channel between two communicating nodes to collect and discover valuable information without disturbing the communication (22; 24; 25).

2. **Active attacks** : active attacks (such as node replication attacks, sybil attacks, wormhole attacks, and compromised node attacks) can be further classified into two categories: external attacks and internal attacks. In external attacks (such as sybil attacks and wormhole attacks), a node does not belong to a sensor network and it can first eavesdrop on packets sent or received by normal participating nodes for the eventual purpose of malicious tempering, interfering, guessing, or spamming, and then injects invalid packets to disrupt the network functionalities.

    - For sybil attacks, a sensor node can illegitimately claim multiple IDs by either directly forging false IDs, or else impersonating legal IDs. This harmful attack may lead to serious threats to distributed storage, routing algorithm and data aggregation.
    - For wormhole attacks, the malicious node may be located within transmission range of legitimate nodes while legitimate nodes are not themselves within transmission range of each other. Thus, the malicious node can tunnel control traffic between legitimate nodes and nonexistent links which in fact are controlled by the malicious node. Finally, the malicious node can drop tunnelled packet or carry out attacks on routing protocols.

    Internal attacks (such as node replication attacks and node compromised attacks) are usually caused by compromised members who are belong to the sensor network in question, and hence internal attacks are more difficult to safeguard against than external attacks.

    - For node replication attacks, when a sensor node is compromised by attackers, they can directly place many replicas of this compromised node at different areas within the networks. Thus, attackers may use these compromised nodes to subvert the network functionalities, for example by injecting false sense data.
    - For compromised attacks, due to the lack of tamper resistance in sensor nodes, attackers may compromise a sensor node and use it to establish communication channels with non-compromised sensors to launch other more serious attacks within the sensor network.

According to the above description of the security threats, we can infer that a secure sensor network corresponds with the following requirements.

1. **Node authentication** : For this requirement, a deployed sensor node proves its validity to its neighboring sensors and the manger node. Thus, an invalid outsider would be unable to send malevolent data into the networks and the manager node can confirm that received sensed data has come from a valid sensor node, not from malicious outsiders. This also implies that a sensor node joined in WSNs has been authenticated and it has the right to access the sensor network.
2. **Availability** : The availability of the network should not be affected even if sensors can only provide limited storage, limited power, and limited computational ability. Therefore, a mechanism regulating of sleep patterns is necessary for a sensor to extend its lifetime.

3. **Location awareness** : The damage cannot be spread from the victimized area to the entire network by security attacks even if the sensor node is compromised. A secure communication scheme must limit the damage's scope caused by the intruders; the mechanism of location awareness is used for this purpose.
4. **Key establishment** For sensor-to-sensor key establishment, a shared key is established by two communication nodes to protect communications. Thus, all sensed data transmitted between participants could be verified and protected even if an attacker eavesdrops on the communications between nodes or injects illegal sensed data into networks, this requirement still provides an adequate level of security.
5. **No verification table** : The verification tables are not required to be stored inside the manager nodes to prevent stolen-verifier attacks.
6. **Confidentiality** : Path-key establishment in every session must be secure against malicious intruders even if those attackers collect transmission packets.
7. **Perfect forward secrecy** : In a two-party path-key establishment, a scheme is said to have perfect forward secrecy if revealing of the secret key to an intruder cannot help him/her derive the session keys of past sessions.
8. **Key revocation** : When the back-end system or the manager node decides to terminate a sensor utilizing task, or when a sensor is lost, the sensor must not be allowed to make use of the credential which it stores to connect to networks.
9. **Re-keying** : By introducing a re-keying mechanism, a manager node can conveniently update a sensor's credential without the intervention of back-end system for the purpose of reducing the communication interactions and management burden on that back-end system.

4. Literature Classifications

There are many researches about the application with key management proposed in the past. In this chapter, we classify wireless sensor network schemes into different classifications based on the application scenarios, including: deployment, organization, re-keying, cryptography and authentication. We then divide each classification into several subclassifications based on key management and node authentication. WSNs have a vast field of applications, including deployment and organization in both military and civilian aspects, from the battlefield surveillance, environment monitoring, medical sensing, traffic control and so on. Thus, the adoptions of security countermeasures are important issues and key management mechanisms are the core of the secure communications. Table 1 is showed the literature classification on secure communication schemes.

4.1 Deployment and Organization of WSNs

Depending on its applications, a sensor deployment manner can be classified in two types: scattered deployment and deployment in designated area. For scattered deployment, in order to achieve large scale of deployment, sensor nodes can be deployed via aerial scattering and the immediate neighboring nodes of any sensor node are unknown in advance. On the other hand, due to the unattended nature of WSNs, an attacker may launch various security threats such as node compromised attacks, the damage might be spread from the compromised area to the entire network. Therefore, many schemes deploy sensors in designated area in order to minimize and localize its impact to a small region.

Classification	Characteristic	Papers
Deployment	Scattered deployment	(1–3; 7; 9; 14; 15; 18; 33; 36; 37; 41–44)
	Designated area	(5; 6; 16; 21; 23; 26; 32; 37; 41; 42)
Organization	Distributed WSN	(1–3; 7; 9; 16; 18; 26; 36; 37; 41–44)
	Hierarchical WSN	(5; 6; 14; 15; 21; 23; 32; 33; 37; 41; 42)
Re-keying	Periodical update	(18; 23; 32; 37; 41; 42; 44)
	Node revocation/attachment	(1; 3; 6; 15; 17; 18; 23; 26; 33; 37; 41–43)
Cryptography	Symmetric key	(1; 3; 5–7; 14–16; 21; 23; 26; 32; 33; 36; 37; 41; 42; 44)
	Asymmetric key	(2; 14; 17; 23; 33; 37; 41–43)
	Hashing function	(3; 7; 15; 17; 18; 23; 32; 35–37; 41; 42; 44)
Authentication	Pair-wise authentication	(1; 3; 5–7; 15–17; 23; 26; 32; 33; 36; 37; 41–44)
	Group-wise authentication	(2; 14; 18; 21; 32; 33; 37; 41; 42; 44)

Table 1. The classification of secure communication schemes

In Figure 1, two general organizations for distributed and hierarchical WSNs are illustrated. A distributed/hierarchical structure of WSN consists of three types of participants, namely, a powerful back-end data center, manager nodes and sensor nodes. Each manager node is responsible for collecting and forwarding all sensed data of its managed area to the back-end data center for further processing from sensor nodes under the area for which it is responsible. In distributed WSNs, a number of sensors are uniformly distributed into sense field and there are no specific roles for each deployment sensor node. In hierarchical WSNs, there are two types of roles for deployment sensors, namely: cluster head and sensor node. Based on geographical and deployment knowledge, a manager node groups all sensors into multiple logical groups and the grouping function is conducted through the selection of cluster head for each group. The main objective of cluster heads are acting as aggregation nodes and fusing the sense data collected from their nearby sensor nodes before routing the resultant data to a manager node. Therefore, cluster heads are much more computational and communication ability than normal sensor nodes in hierarchical WSNs.

4.2 Authentication Scenarios

For authentication in WSNs, three types of scenarios for pair-wise and group-wise authentication are illustrated in Figure 2. For example, in Figure 2(a), a pair-wise authentication is accomplished between node x and node y. For group-wise authentication, we divided it into two scenarios: cluster-based authentication and global-based authentication. In Figure 2(b), a cluster authentication is used by a cluster head and all its neighboring sensor nodes, and it

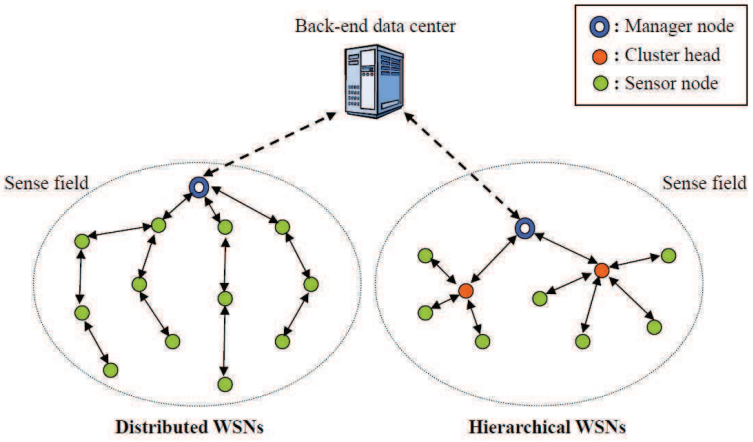


Fig. 1. Organization of WSNs

is used for securing clustered broadcast messages. Finally, in Figure 2(c), this is a node authentication verified by the manager node and all sensor nodes in the sense field. A global authentication is done by the manager node for securing communications that are broadcast to the entire network and prevent illegal sensor nodes from participating the sensor networks.

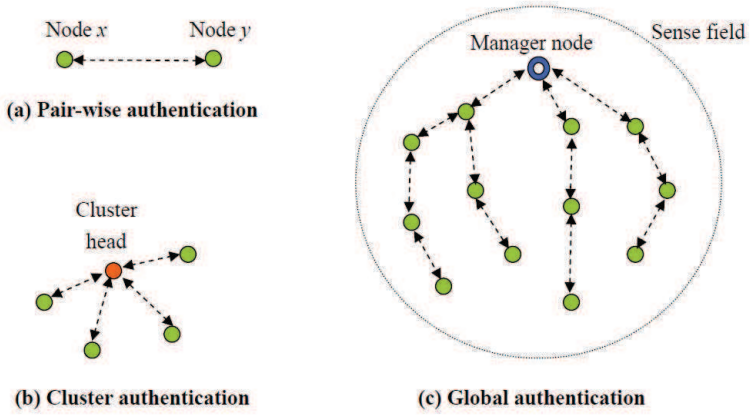


Fig. 2. Authentication scenarios

4.3 Cryptographic Approaches

In order to protect privacy and secure communications, participating nodes joined in WSNs should be authenticated and shared keys should be established between deployed sensors and their neighboring nodes. For example, in two-party communications, a deployed node establishes a pair-wise key with each of its neighboring nodes. Similarly, in broadcast communications, a group-wise key should be shared by all nodes in the network. We classify the

security of node authentication and key establishment schemes into three types of cryptography: symmetric keys, asymmetric keys and one-way hashing functions.

4.3.1 Symmetric Keys

Recently, many schemes (1; 3; 5–7; 14–16; 21; 23; 26; 32; 33; 36; 37; 41; 42; 44) were proposed to secure communications in WSNs and one of secure communication schemes is based on symmetric key cryptography. A simple solution to ensure privacy would be store a single master key MK into all deployed sensors prior to their deployment. Thus, a legal node N_A can use this master key to establish a pair-wise key $K = F(MK||N_A||N_B)$ with its neighboring node N_B for securing communications that require privacy or node authentication, where F is a pseudo-random function. However, this solution fails to prevent security breaches and thus is impracticable for WSNs for whose sensors lack tamper resistance and are easy for attackers to compromise, leaving all the secret in those networks known to attackers. As a result, during initial deployment phase, we suggest that there should be a security mechanism for erasing master key. For example, the manager node sets a timer with reasonable time interval T for a deployed sensor to discover its neighboring nodes. When a timer expires after T, deployed sensor node erases MK and attackers cannot inject illegal sensed data into networks without knowing MK.

The other extreme solution is to store a set of $n-1$ key pairs in each sensor node before deployment in such a way that it shares a unique key pair with all other nodes in the networks, where n is the number of sensor nodes in WSNs. However, this solution is only suitable for small networks due to it requires large memory to store keys and becomes a serious problem when the network needs to be expanded. Therefore, many probabilistic key pre-deployed schemes were proposed to overcome these shortages. A large pool of P keys and their identifiers are generated and d distinct keys are randomly drawn from P and pre-loaded into each sensor's key ring, where $P \gg d$. This solution ensures that only a few keys need to be stored in each sensor's memory and two nodes share at least one key, based on a selected probability. An extension to the basic probabilistic scheme is proposed by Liu and Ning, called polynomial pool-based key pre-distribution scheme (26). This scheme randomly selects polynomials from a polynomial pool and stores them to each sensor instead of randomly choosing keys from a key pool. A detailed survey on symmetric keying schemes could be found in (37; 41; 42)

4.3.2 Asymmetric Keys

As sensors have constrained resources and are expensive to install, computational and communication overhead must be kept at a minimum. Hence the traditional asymmetric cryptosystems such as RSA (34) and ElGamal (10) are not suitable to use in WSNs and most key management and establishment schemes for WSNs are based upon symmetric key cryptography. However, many security solutions based on symmetric keys are usually subject to various attacks and they are unable to achieve sufficient scalability (2). On the contrary, asymmetric key cryptography provide better scalability and security strength and allow for flexible key management as it does not require pre-distribution of keys. Therefore, several solutions based on asymmetric key algorithms have been proposed in the literature (2; 14; 17; 23; 33; 37; 41–43). Gura et al. (12) showed that both RSA and Elliptic Curve Cryptography (ECC) (20) public key cryptography (PKC) is applicable on two 8-bit CPUs without hardware acceleration and ECC is widely being adopted to provide PKC support so that the existing PKC-based solutions can be exploited. TinyECC(27), a software package, is being investigated to provide ECC-based PKC operations that can be flexibly configured and integrated into limited-resource sensor

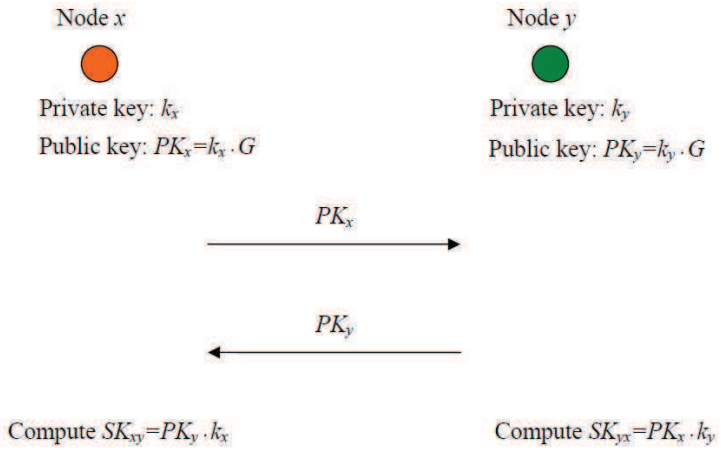


Fig. 3. Key exchange of a agreed pair-wise key under Diffie-Hellman based on ECDLP

devices. Targeted at security of TinyECC, it provides PKC-based schemes that have proven to be secure; ECC-160 and ECC-224 have the same security level as RSA-1024 and RSA-2048, respectively. Moreover, at the beginning of the node deployment, two nodes establish the permanent pair-wise key using a computationally less expensive variant of the Diffie-Hellman key exchange scheme (8) based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) (11; 28), as shown in Figure 3. Each node is pre-loaded with private/public key pair and only two rounds of handshake are required. Private keys are denoted as k_x and k_y for node x and node y, respectively as well as the public keys $PK_x = k_x \cdot G$ and $PK_y = k_y \cdot G$. After receiving neighboring node's public key, each node will compute agreed pair-wise key as $SK_{xy} = PK_y \cdot k_x = k_x \cdot k_y \cdot G = PK_x \cdot k_y = SK_{yx}$.
In 2007, Zhou et al. design an access control scheme (43) based on ECC for sensor networks and their scheme accomplishes node authentication and key establishment to prevent malicious nodes from joining sensor networks. In 2009, Huang proposed an improved version (17) of Zhou et al.'s scheme to reduce large amounts of computations and communications between two nodes. In (14), Hsieh et al. proposed a dynamic authentication protocol to authentication a new node-joining sensor network, establishment of secure links and broadcast authentication between neighboring nodes in cluster-based sensor networks. In (2), Cao et al. proposed an ID-based multi-user broadcast authentication scheme based on ECC for providing strong security, sound scalability and performance efficiency simultaneously.

4.3.3 One-way Hashing Functions

One-way hashing functions (such as MD5 and SHA-1) are important tools in the field of cryptographic applications due to their efficiency with regard to computational costs and are suitable for resource-constrained devices. In general, the security of an one-way hashing function $h(.)$ is based on the hardness of inverting the inputs from the outputs; that is, given a and $h(.)$, it is easy to compute $h(a) = b$. However, only given b, it is hard to find a, satisfying $h(a) = b$. Figure 4 shows the construction of an one-way hash chain. Participating nodes generate an initial value $h^1(k) = h(k)$, where k is the initial key and $h^1(k)$ represents the initial key k has been hashed once. Thus, h^n can be regarded as the key k which has been hashed n times such

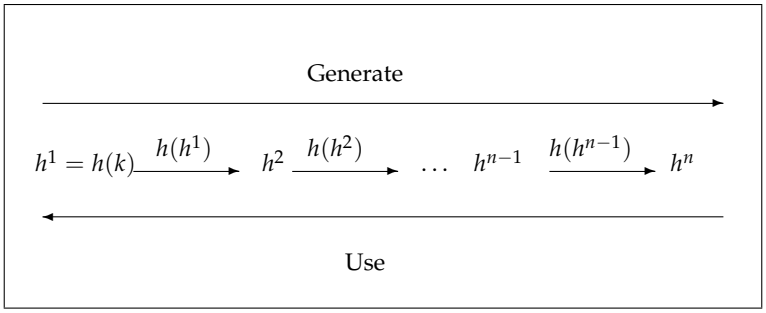


Fig. 4. Construction of an one-way hash chain

that $h^n(k) = h(h^{n-1}(k))$, where $n = 2, 3, 4, \ldots$. Due to the one-way property, the hash chain can be used in reverse order of generation for authentication; that is, $h^{n-1}(k)$ can be proven to be authentic if $h^n(k)$ has been proven to be authentic. For example, we assume that the lifetime of a sensor network is divided into n intervals and each time interval T_m has its own master key $K_m = h(K_{m-1})$, where $1 \leq m \leq n$, $K_1 = h(k)$ and k is an initial key. Figure 5 illustrates the mapping between master keys and time intervals.

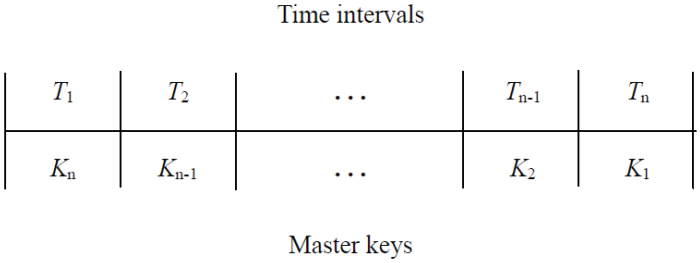


Fig. 5. The mapping between master keys and time intervals by using one-way hash chain

In addition, the Message Authentication Code (MAC) which is generated by node x and it would be verified by node y and is defined by $MAC = h(k; m)$, where m denotes the message under the protection key of k. Several solutions based on one-way hashing functions have been proposed in the literature (3; 7; 15; 17; 18; 23; 32; 35–37; 41; 42; 44). In (35), Shan and Liu proposed the hashed random key pre-distribution, if nodes x and y are deployed in WSNs, respectively, with $K_x = h^a(k)$ and $K_y = h^b(k)$, then node y can easily derive $K_x = h^{a-b}(K_y)$, where k is randomly selected from the key pool and $a > b$. In Li et al.'s scheme (23), the concepts of MAC and one-way hash chain are widely be used to authenticate the validity of transmission messages and participating nodes.

5. Conclusions and Future Works

We argue that no single security scheme is ideal to all the applications where sensor networks are used and the cryptographic techniques adopted must depend upon the scenarios of ap-

plied architectures and concerns of security requirements in WSNs. There are some future research issues should be considered for wireless sensor networks in this chapter. There are also the critical success factors of wireless sensor networks. We briefly describe them as follows.

- **Soft message encryption**: In order to achieve performance efficiency and reduce resource requirements, a soft message encryption mechanism is used in which a message is divided into different parts and each part of the message is involved in encrypting the whole message itself. This technique has less strength than the sophisticated encryption algorithms. However, it eliminates the need of key distribution centers and key establishment (29). For soft message encryption (13), we assume that a $3m$-bits message is divided into three parts of m bits each and we define these parts by x, y and z. Then, parts x, y and z are encrypted by the following conditions:

  $$x' = x \oplus z$$
  $$y' = y \oplus x$$
  $$z' = z \oplus x \oplus y$$

  Now, the parts x', y' and z' are now transmitted instead of x, y and z. Finally, at the back-end data center, the message parts can be decrypted using the following equations:

  $$x = x' \oplus y' \oplus z'$$
  $$y = x' \oplus z'$$
  $$z = y' \oplus z'$$

- **Multiple communication paths**: For pair-wise key establishment in single communication path, it is vulnerable to stop forwarding attack if an intermediate node is compromised along the path. Moreover, it cannot prevent Byzantine attacks that attackers may use the compromised nodes to alter, inject, spoof, or sniff messages. A secret key may be exposed if any intermediate node along the path is compromised and a secret key established between the source node and destination node by multiple communication paths can decrease the risk of path key exposure problem. Therefore, multi-path key establishment solutions are resilient to resist stop forwarding, ensure network availability from connective failure and prevent compromised sensors from knowing the secret in WSNs (30; 36; 38). In Figure 6, we use the above-mentioned soft encryption with multiple communication paths as an example.
- **Efficient data aggregation**: The main objective of data aggregation technique is to combine the sensed data receiving from deployed sensor nodes at certain cluster heads to minimize the total amount of data transmission before forwarding sensed data to the external manager node. An efficient and secure data aggregation is essential for cluster-based WSNs in which data aggregation is eliminating data redundancy to reduce energy consumption to extend the network lifetime (4; 19; 31; 39; 40). An example of data aggregation is presented in Figure 7 where a group of data aggregators collect the data from their neighboring nodes, aggregate them and send the aggregated data to the manager node.
- **Malicious node detection**: In order to ensure a secure networking, it should design a security mechanism to detect malicious nodes and false messages by legitimate nodes

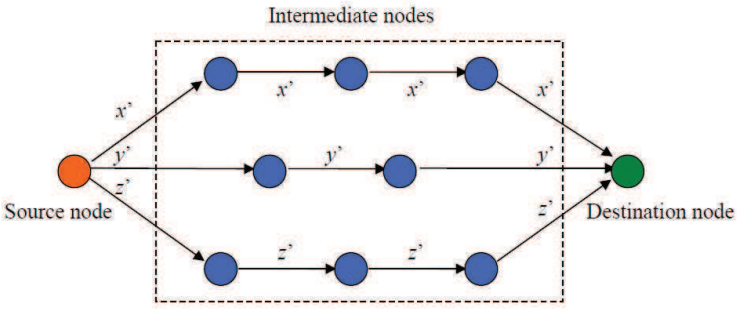


Fig. 6. An example of multiple communication paths

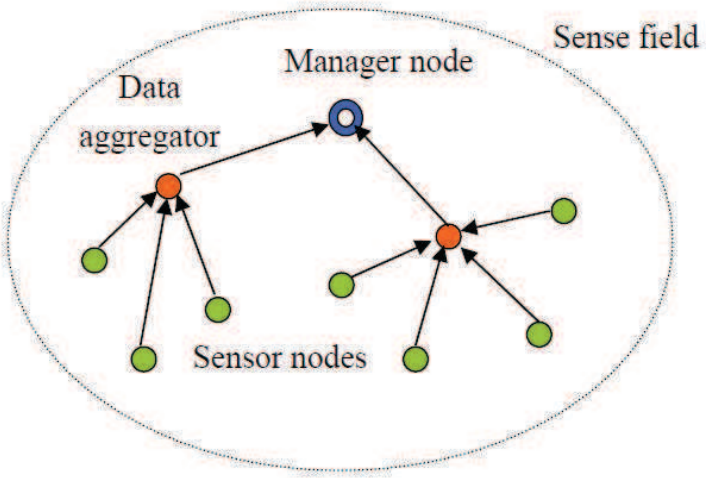


Fig. 7. Data aggregation in cluster-based wireless sensor networks

and the basic idea of detection of malicious behavior node is to provide a hop-by-hop authentication in WSNs.

- **Node revocation-awareness**: Unlike the addition of a sensor node to WSNs, the revocation of a node is much more complicated. When a sensor node is compromised or it exhausts its power, it must not be allowed to make use of the key information stored in local memory to connect to the sensor networks and it requires many keys to be revoked. As a result, it is important to design a node revocation-awareness mechanism without bring serious impacts on the network efficiency and connectivity.

6. References

[1] Sasikanth Avancha, Jeffrey Undercoffer, Anupam Joshi and John Pinkston, “Secure sensor networks for perimeter protection", *Computer Networks*, vol. 43, no. 4, pp. 421-435, 2003.

[2] Xuefei Cao, Weidong Kou, Lanjun Dang and Bin Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks", *Computer Communications*, vol. 31, no. 4, pp. 659-667, 2008.
[3] Haowen Chan, Virgil D. Gligor, Adrian Perrig and Gautam Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks", *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 3, pp. 233-247, 2005.
[4] Huifang Chen, Hiroshi Mineno and, Tadanori Mizuno, "Adaptive data aggregation scheme in clustered wireless sensor networks", *Computer Communications*, vol. 31, no. 15, pp. 3579-3585, 2008.
[5] Yi Cheng and Dharma P. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks", *Ad Hoc Networks*, vol. 5, no. 1, pp. 35-48, 2007.
[6] Michael Chorzempa, Jung-Min Park and Mohamed Eltoweissy, "Key management for long-lived sensor networks in hostile environments", *Computer Communications*, vol. 30, no. 9, pp. 1964-1979, 2007.
[7] Mauro Conti, Roberto Di Pietro and Luigi V. Mancini, "ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks", *Ad Hoc Networks*, vol. 5, no. 1, pp. 49-62, 2007.
[8] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.
[9] E. Ekici, S. Vural, J. McNair and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks", *Ad Hoc Networks*, vol. 6, no. 2, pp. 195-209, 2008.
[10] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Transactions on Information Theory*, vol. IT-31, no. 4, pp. 469-472, 1985.
[11] A. Riskiran and R. Lee, "Workload characterization of elliptic curve cryptography and other network security for constrzined environments", *in Proceedings of IEEE International Workshop on Workload Characterization*, pp. 127-137, 2002.
[12] N. Gura, A. Patel, A. Wander, H. Eberle and S. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit cpus", *In 2004 Workshop on Cryptographic Hardware and Embedded Systems*, August 2004.
[13] T. Haniotakis, S. Tragoudas and C. Kalapodas, "Security enhancement trhough multiple path transmission in ad hoc networks", *in IEEE International Conference on Communiations*, pp. 4187-4191, 2004.
[14] Meng-Yen Hsieh, Yueh-Min Huang and Han-Chieh Chao, "Adaptive security design with malicious node detection in cluster-based sensor networks", *Computer Communications*, vol. 30, no. 11-12, pp. 2385-2400, 2007.
[15] Fei Hu, Waqaas Siddiqui and Krishna Sankar, "Scalable security in Wireless Sensor and Actuator Networks (WSANs): Integration re-keying with routing", *Computer Networks*, vol. 51, no. 17, pp. 285-308, 2007.
[16] D. Huang and D. Medhi, "Secure pairwise key establishment in large-scale sensor networks: an area partitioning and multigroup key predistribution approach", *ACM Transactions on Sensor Networks*, vol. 3, no. 3, article 16, 2007.
[17] H. F. Huang, "A novel access control protocol for secure sensor networks", *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 272-276, 2009.

[18] Yixin Jiang, Chuang Lin, Minghui Shi and Xuemin (Sherman) Shen, "Self-healing group key distribution with time-limited node revocation for wireless sensor networks", *Ad Hoc Networks*, vol. 5, no. 1, pp. 14-23, 2007.
[19] Jamal N. Al-Karaki, Raza Ul-Mustafa and Ahmed E. Kamal, "Data aggregation and routing in Wireless Sensor Networks: Optimal and heuristic algorithms", *Computer Networks*, vol. 53, no. 7, pp. 945-960, 2009.
[20] K. Koblitz, "Elliptic Curve Cryptosystems", *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.
[21] Jason H. Li, Bobby Bhattacharjee, Miao Yu and Renato Levy, "A scalable key management and clustering scheme for wireless ad hoc and sensor networks", *Future Generation Computer Systems*, vol. 24, no. 8, pp. 860-869, 2008.
[22] Chun-Ta Li, Min-Shiang Hwang and Yen-Ping Chu, "Improving the Security of A Secure Anonymous Routing Protocol with Authenticated Key Exchange for Ad Hoc Networks", *International Journal of Computer Systems Science and Engineering*, vol. 23, no. 3, pp. 227-234, 2008.
[23] Chun-Ta Li, Min-Shiang Hwang and Yen-Ping Chu, "An Efficient Sensor-To-Sensor Authenticated Path-Key Establishment Scheme for Secure Communications in Wireless Sensor Networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, 2009.
[24] Chun-Ta Li and Yen-Ping Chu, "Cryptanalysis of Threshold Password Authentication Against Guessing Attacks in Ad Hoc Networks", *International Journal of Network Security*, vol. 8, no. 2, pp. 166-168, 2009.
[25] Chun-Ta Li, Min-Shiang Hwang and Yen-Ping Chu, "A Secure Event Update Protocol for Peer-To-Peer Massively Multiplayer Online Games Against Masquerade Attacks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 12(A), pp. 4715-4723, 2009.
[26] D. Liu and P. Ning, "Improving Key Predistribution with Deployment Knowledge in Static Sensor Networks", *ACM Transactions on Sensor Networks*, vol. 1, no. 2, pp. 204-239, 2005.
[27] An Liu and Peng Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks", *Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN 2008)*, 2008.
[28] D. Malan, M. Welsh and M. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography", *in Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, pp. 71-80, 2004.
[29] Prayag Narula, Sanjay Kumar Dhurandher, Sudip Misra and Isaac Woungang, "Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing", *Computer Communications*, vol. 31, no. 4, pp. 760-769, 2008.
[30] Nidal Nasser and Yunfeng Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", *Computer Communications*, vol. 30, no. 11-12, pp. 2401-2412, 2007.
[31] Suat Ozdemir and Yang Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview", *Computer Networks*, vol. 53, no. 12, pp. 2022-2037, 2009.
[32] Biswajit Panja, Sanjay Kumar Madria and Bharat Bhargava, "A role-based access in a hierarchical sensor network architecture to provide multilevel security", *Computer Communications*, vol. 31, no. 4, pp. 793-806, 2008.

[33] Rabia Riaz, Ayesha Naureen, Attiya Akram, Ali Hammad Akbar, Ki-Hyung Kim and H. Farooq Ahmed, "A unified security framework with three key management schemes for wireless sensor networks", *Computer Communications*, vol. 31, no. 18, pp. 4269-4280, 2008.

[34] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[35] T. Shan and C. Liu, "Enhancing the key pre-distribution scheme on wireless sensor networks", *in IEEE Asia-Pacific Conference on Service Computing*, IEEE CS, pp. 1127-1131, 2008.

[36] Jang-Ping Sheu and Jui-Che Cheng, "Pair-wise path key establishment in wireless sensor networks", *Computer Communications*, vol. 30, no. 11-12, pp. 2365-2374, 2007.

[37] Marcos A. Simplicio Jr., Paulo S.L.M. Barreto, Cintia B. Margi and Tereza C.M.B. Carvalho, "A survey on key management mechanisms for distributed Wireless Sensor Networks", *Computer Networks*, article in press, 2010.

[38] Eliana Stavrou and Andreas Pitsillides, "A survey on secure multipath routing protocols in WSNs", *Computer Networks*, vol. 54, no. 13, pp. 2215-2238, 2010.

[39] S. Upadhyayula and S. K. S. Gupta, "Spanning tree based algorithms for low latency and energy efficient data aggregation enhanced convergecast (DAC) in wireless sensor networks", *Ad Hoc Networks*, vol. 5, no. 5, pp. 626-648, 2007.

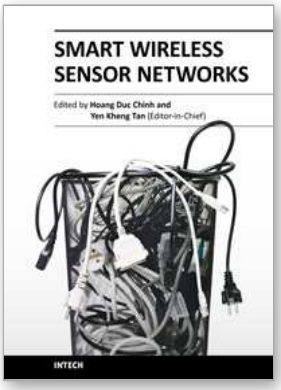
[40] Kui Wu, Dennis Dreef, Bo Sun and Yang Xiao, "Secure data aggregation without persistent cryptographic operations in wireless sensor networks", *Ad Hoc Networks*, vol. 5, no. 1, pp. 100-111, 2007.

[41] Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu and Michael Galloway, "A survey of key management schemes in wireless sensor networks", *Computer Communications*, vol. 30, no. 11-12, pp. 2314-2341, 2007.

[42] Junqi Zhang and Vijay Varadharajan, "Wireless sensor network key management survey and taxonomy", *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63-75, 2010.

[43] Yun Zhou, Yanchao Zhang and Yuguang Fang, "Access control in wireless sensor networks", *Ad Hoc Networks*, vol. 5, no. 1, pp. 3-13, 2007.

[44] S. Zhu, S. Setia and S. Jajodia, "LEAP+: Efficient seurity mechanisms for large-scale distributed sensor networks", *ACM Transactions on Sensor Networks*, vol. 2, no. 4, pp. 500-528, 2006.



Smart Wireless Sensor Networks

Edited by Yen Kheng Tan

ISBN 978-953-307-261-6
Hard cover, 418 pages
Publisher InTech
Published online 14, December, 2010
Published in print edition December, 2010

The recent development of communication and sensor technology results in the growth of a new attractive and challenging area â€“ wireless sensor networks (WSNs). A wireless sensor network which consists of a large number of sensor nodes is deployed in environmental fields to serve various applications. Facilitated with the ability of wireless communication and intelligent computation, these nodes become smart sensors which do not only perceive ambient physical parameters but also be able to process information, cooperate with each other and self-organize into the network. These new features assist the sensor nodes as well as the network to operate more efficiently in terms of both data acquisition and energy consumption. Special purposes of the applications require design and operation of WSNs different from conventional networks such as the internet. The network design must take into account of the objectives of specific applications. The nature of deployed environment must be considered. The limited of sensor nodesâ€™ resources such as memory, computational ability, communication bandwidth and energy source are the challenges in network design. A smart wireless sensor network must be able to deal with these constraints as well as to guarantee the connectivity, coverage, reliability and security of networkâ€™s operation for a maximized lifetime. This book discusses various aspects of designing such smart wireless sensor networks. Main topics includes: design methodologies, network protocols and algorithms, quality of service management, coverage optimization, time synchronization and security techniques for sensor networks.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Chun-ta Li (2010). Security of Wireless Sensor Networks: Current Status and Key Issues, Smart Wireless Sensor Networks, Yen Kheng Tan (Ed.), ISBN: 978-953-307-261-6, InTech, Available from: http://www.intechopen.com/books/smart-wireless-sensor-networks/security-of-wireless-sensor-networks-current-status-and-key-issues

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820

Fax: +385 (51) 686 166
www.intechopen.com

Fax: +86-21-62489821

© 2010 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License, which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.