The Annals of "Dunarea de Jos" University of Galati
Fascicle I – 2009. Economics and Applied Informatics. Years XV - ISSN 1584-0409

A Framework for Secure and Survivable Wireless Sensor Networks

Mi Chaw Mon THEIN
Thandar THEIN
thandartheinn@gmail.com
University of Computer Studies, Yangon, Myanmar

Abstract. Wireless sensor networks increasingly become viable solutions to many challenging problems and will successively be deployed in many areas in the future. A wireless sensor network (WSN) is vulnerable to security attacks due to the insecure communication channels, limited computational and communication capabilities and unattended nature of sensor node devices, limited energy resources and memory. Security and survivability of these systems are receiving increasing attention, particularly critical infrastructure protection. So we need to design a framework that provide both security and survivability for WSNs. To meet this goals, we propose a framework for secure and survivable WSNs and we present a key management scheme as a case study to prevent the sensor networks being compromised by an adversary. This paper also considers survivability strategies for the sensor network against a variety of threats that can lead to the failure of the base station, which represents a central point of failure.

Keywords: key management scheme, security, survivability, WSN

JEL Code: D80, D85

1. Introduction

A wireless sensor network typically consists of a number of small autonomous sensing devices, each of which is called a sensor node with a power unit, a sensing unit, a processing unit, a storage unit and a wireless transmitter/receiver. Applications of WSNs are numerous and growing, and range from indoor deployment scenarios in the home and office to outdoor deployment scenarios in natural, military and embedded settings. The sensor nodes can be deployed in controlled environment such as factories, homes, or hospitals; they can also be deployed in uncontrolled environment such as a disaster or hostile area, and dangerous environment such as battlefields, toxic regions etc [1].

Wireless sensor network are vulnerable to security attacks due to the broadcast nature of transmission and the limited computation and communication capabilities of the sensor node [8]. Moreover the majority of the WSN applications should be run continuously and reliably without interruptions. Hence, survivability implies that networks should have the capability to operate under node failures and attacks. On the other hand, security encompasses the aspects of confidentiality, authentication, and integrity of the application information. Obviously, security and survivability in WSNs face many common challenges, ranging from the wireless nature of communications, resource limitations on sensor nodes, very large and dense networks, and unknown network topology prior to deployment, to high risk of physical attacks to unattended sensors [6]. To meet this goals, we focus on not only the security mechanisms but also the survivable mechanisms of wireless sensor networks.

The survivability of sensor networks can be achieved by several ways. The security mechanisms in sensor networks such as encryption algorithms, key management, and authentication are most important of defense. There is an interaction between security and survivability. So, we need to study the coupling between security and survivability, and a need to create design strategies consist with both sets of requirements for WSN.

To provide secure communications for the WSNs, all the messages should be encrypted and authenticated. Consequently, it is important to design strong and efficient key distribution mechanisms for WSNs. Clearly, using a single shared key in the whole WSN is not a good idea because an adversary can easily obtain the key . Therefore, as a fundamental security service, pair-wise key establishment shall be used, which can enable the sensor nodes to communicate securely with each other using cryptographic techniques.

However, due to resource constraints on sensor nodes, it is not feasible for sensors to use traditional pair-wise key establishment techniques such as public key cryptography and key distribution center. In this paper, we present a comprehensive study on security and survivability for WSNs. Our goals is to develop a framework, secure and survivable WSNs, that provides security and survivability measures that are available for critical services in spite of physical and network based security attacks, accidents, or failures. We first study the requirements of both security and survivability.

The remainder of this paper is organized as follows. Section 2 introduces related work on WSNs security and survivability. Section 3 describes Sensor Network Architecture and Environment. Section 4 discusses the security and survivability requirements for the sensor networks. Section 5 presents a proposed framework and also describes secure key management scheme as a case study. Finally, Section 6 concludes the paper.

2. Related Work

There are a lot of survey on security for wireless sensor networks. In this paper, we introduce some relevant survey papers here. For securing a wireless sensor network, Mayank [2] introduced sensor networks, its related security problems, threats, risks and characteristics, and a brief introduction to SPINS, TinySec and LEAP. Mona et al. [3] discussed a concise survey on sensor network constraints, security requirements, attacks and defensive measures. They described that security requirements are critical to preventing an adversary from compromising the security of a distributed wireless sensor networks and the key establishment protocols and approaches for distributed wireless sensor networks must satisfy several security and functional requirements. Moreover, they also revealed that for security, there are many defensive measures for protecting the sensor networks from attacks: key establishment in WSNs, 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.

The authors [4] presented a security framework for wireless sensor network which is composed of three phases: cluster formation, secure key management scheme and secure routing. Zia et al. [5] presented a secure triple-key management scheme which provides stronger resilience against susceptible attacks on sensor networks by keeping in mind the resource starved nature of sensor nodes. They only focus on security of WSNs.

An optimal key management model to provide security and survivability for heterogeneous wireless sensor networks is presented in [7]. This key management scheme can balance the cost of the sensor network and maximize the resilience of the sensor network with the required security key connectivity constraint in different hostile environment, with a small percentage of the powerful sensor nodes. Qin et al. [6] presented the design issues for secure and survivable wireless sensor networks, which are vulnerable to physical and network security attacks accidents, and failures. They observed that a good design can improve both security and survivability of hetegenerous wireless sensor network. But there is a little study on the coupling between security and survivability for wireless sensor networks.

3. Sensor Network Architecture and Environment

In this section we introduce the sensor network characteristics on which our security and survivability architecture is based. Three groups of aspects have a direct impact on the design of our architecture: the sensor nodes characteristics, the network characteristics, and the environment.

3.1. Sensor Nodes

Sensor node typically consists of the five components: sensing unit, analog-to-digital convector (ADC), central processing unit (CPU), power unit, and communication unit. They are assigned with different tasks. The sensor unit is responsible for collecting information as the ADC requests, and returning the analog data it sensed. ADC is a translator that tells the CPU what the sensor unit has sensed, and also informs the sensor unit what to do. Communication unit is tasked to receive command or query from, and transmit the data from CPU to the outside world. CPU is the most complex unit. It interprets the command or query to ADC, monitors and controls power if necessary, processes received data, computes the next hop to the sink, etc. Many other units may be added for special usage, but the above five units are the most important ones and are included in every sensor node.

The sensor nodes are characterized as severely resource-constraint devices in terms of available energy, memory, and computational power. Different types of sensors such as seismic, magnetic, thermal, visual, infrared, acoustic and radar are used to monitor a wide variety of ambient condition viz. temperature, pressure, humidity, vehicular movement, and noise level. The sensor nodes are not tamper-proof, due to cost factors and the general difficulty in building such devices. Consequently, it is possible to physically manipulate the devices if captured. For interaction purposes, the nodes are equipped with radio frequency communication capabilities. However, this wireless communication provides only limited bandwidth. These sensor node-specific factors set several constraints for the security architecture. Due to the limited bandwidth and communication being the most expensive operation in terms of energy, messages should not be extended significantly in length when apply security and survivability services.

3.2. Sensor Network

WSNs are autonomous system consisting of tiny sensors that are equipped with integrated sensing, general purpose computing and limited range or transmitting capabilities. A notable feature of the architecture of a WSN is its hierarchy, rooted in a base station. In most of the applications sensors are required to detect events and then communicate the collected information to a distant base station (BS). In the hierarchical network architecture, WSN is divided into several clusters. In each cluster, one special node acts as cluster head (CH) which collects and compresses the data sent by common sensor nodes within that cluster, and then transmits the processed data to BS.

The main functions of cluster-heads include sensing, collecting data from the common sensor nodes, aggregating the raw data and transferring the processed data to the BS. A cluster based WSN is shown in figure 1. Another important point in sensor networks is the limited lifetime of sensor data. Sensor data and accordingly events that are derived from it should be communicated in real-time. The network characteristics, similar to the node characteristics, determine important aspects of the desired security and survivability architecture.

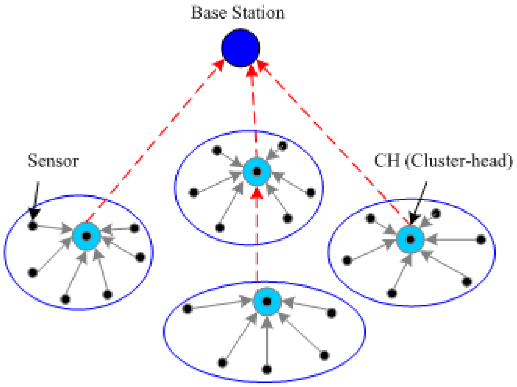

Figure 1. Cluster-based WSN Architecture

3.3. Sensor Environment

The environment of these sensor networks depends on the assigned task. In WSNs, the sensor nodes can be deployed in controlled environment such as factories, homes, or hospitals; they can also be deployed in uncontrolled environment such as disaster or hostile area, in particular battlefield, where monitoring and surveillance is crucial. Clearly, security and survivability in WSNs are extremely important for both controlled environment and uncontrolled and hostile environment.

4. The Architecture for Secure and Survivable WSN

In this section we describe the security and survivability properties required by sensor network and every sensor application should here in order to guarantee appropriate level of security. Survivability can be defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. Security can be defined as the combination of availability, confidentiality, and integrity and focuses on "recognition of attacks" and "resistance of attacks".

4.1 Security Requirements for WSN

The security requirements that constitute fundamental objectives based on which every sensor application should adhere in order to guarantee an appropriate level of security.

Confidentiality: Confidentiality requirement is needed to ensure that sensitive information is well protected and not revealed to unauthorized third parties. The confidentiality objective is required in sensors' environment to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication.

Authentication: As in conventional systems, authentication techniques verify the identity of the participants in a communication, distinguishing in this way legitimate users from intruders. In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really send by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data.

Integrity: Moving on to the integrity objective, there is the danger that information could be altered when exchanged over insecure networks. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications rely on the integrity of the information to function with accurate outcomes.

Freshness: Data freshness objective ensures that messages are fresh, meaning that they obey in a message ordering and have not been reused. One of the many attacks launched against sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network.

Secure Management: Management is required in every system that is constituted from multi components and handles sensitive information. In the case of sensor networks, we need secure management on base station level; since sensor nodes communication ends up at the base station, issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management.

Availability: Availability ensures that services and information can be accessed at the time that they are required. In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks. Lack of availability may affect the operation of many critical real time applications.

The requirement of security not only affects the operation of the sensor network, but also is highly important in maintaining the availability of the whole network [10]. The security requirements that should be met to better protect WSNs from adversaries.

4.2. Survivability Requirements for WSN

This subsection is focused on survivability requirements related with sensor network operation. The majority of the WSN applications should be run continuously and reliable without interruptions. Hence, survivability should also be taken into account in developing WSNs [6]. In the design of survivable WSNs, survivability implies that networks should have the capability to operate under node failures and attacks.

Survivability requirements refer to system capabilities for the delivery of essential services in the presence of attacks and intrusions, and recovery of full services [9]. First, survivability requires that system requirements be organized into essential services and non-essential services, perhaps organized in terms of business criticality. Essential services must be maintained even during successful intrusions; non-essential services are to be recovered after intrusions have been dealt with. Second survivability itself imposes new types of requirements on systems for resistance to, recognition of, and in particular, recovery from intrusions and compromises.

Requirements Definition for Survivability Services

Survivability services can be organized into three general categories, namely: resistance, recognition, and recovery.

Resistance Service Requirements: Resistance refers to the capability of a system to deter attacks.
Recognition Service Requirements: Recognition refers to the capability to recognize attacks or to recognize the probing that may precede attacks.

Recovery Service Requirements: Recovery refers to a system's ability to restore services after an intrusion has occurred and to improve its capability to resist or recognize future intrusion attempts.

4.3. The Architecture

Firstly, we present a general WSN security and survivable architecture. Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, couple with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to 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. Thus, WSNs also have the general security requirements of confidentiality, authentication, integrity, and security management.

The majority of WSN applications should be run continuously and reliably without interruption. Due to resource constraints and uncontrolled environment of WSN these two factors are very important. To increase security and survivability, we propose a general security framework for WSN. To provide secure communications for the WSNs, all aspects of security requirements and services need to be met and provided. Consequently, it is also important to address the reliability issue in the design of secure architecture for WSN using modeling and survivable strategies.

In figure 2, we describe the security and survivablity requirements, the prevention and protection schemes need to be designed and met the security requirements and provide the secure services. The detection and response schemes need to be designed to passively protect WSNs, we use various security techniques for WSN. The security and survivability requirements and services, combined with the security and survivability mechanisms and techniques, form the general security and survivability architecture for WSN.

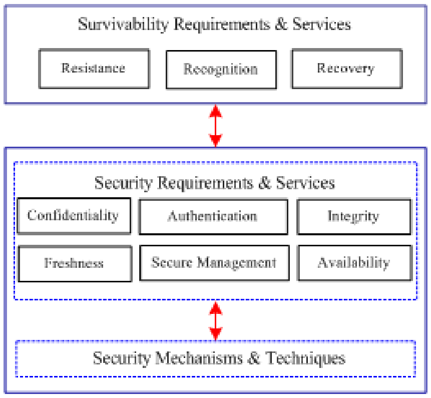

Figure 2. General Architecture for Secure and Survivable WSN

5. Proposed Secure and Survivable Framework

In this section, we address our proposed secure and survivable model for WSN in a UML (Unified Modeling Language) collaboration diagram, as shown figure 3. This diagram consists of nine major components: User, Base Station, Cluster Head, Sensor Node, Registry, Broker, Monitor, Key Management and Factory. The concept of the factory is commonly used design patterns in the object oriented design. Normal operation steps are depicted by the messages from (1.1 to 3.10), and the event of any failures (component, system, sensor node, cluster head or network) security breaches, or attacks on the system, the recovery operation starts with message 4.1 to 4.4. Key management steps are depicted by the messages from (2.1 to 2.4).

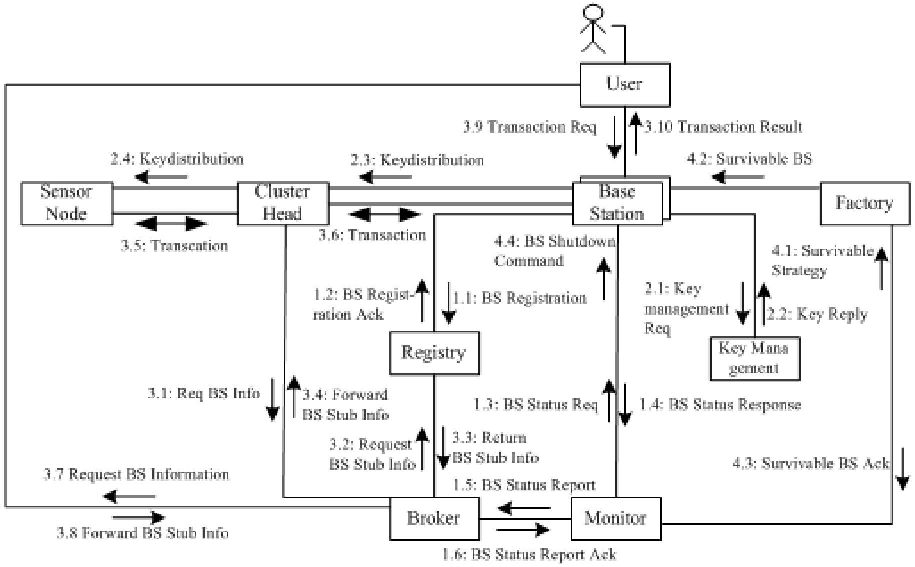

Figure 3. Proposed Model for Secure and Survivable WSN

In order to support secure and survivable services, base station needs additional communication channels among the components. The registry provides a conventional naming service and the redundant base stations are generated and deployed before the operation starts. The base stations register themselves to the registry implying that their service is available. The available base stations list is maintained by the monitor component. The monitor checks the base stations' operating status. The broker acts as an entry point to the service. The user interface and cluster head will connect to the broker asking for a specific service and base station information. The broker keeps a list of active base stations running through the monitor. The list is updated with the monitors' reports. The monitor will respond the base stations status information when it receives the broker's request. The monitors communicate with other monitors' coverage. The monitor performs operations such as gathering the server status report, forwarding it to the broker and, most important, analyzing the reason for failure and the type of attacks in order to find out possible survivable methods.

In the beginning of the operation, an array of 'n' redundant components is initiated. These redundant base stations will be used as a buffer while a more robust base station is generated and deployed. When a base station fails because of an attack or internal failures, the buffer base stations will take over the service for a brief period until the new survivable base station is initialized. Since all of the buffer base stations are susceptible to the same failures or attacks, it is a matter of time before the redundant base stations are also infected by the same reason. Therefore, if the transition period is long, multiple buffer base station may be used before the survivable base station is ready. The monitor informs the factory about the base station failure and requests to build a new survivable base station.

The factory, upon receiving the request from the monitor, starts to build the survivable base station. During the building time the factory deploys a buffer base station to serve user and cluster head for a temporary period. The factory updates the active base station list to the monitor, and the monitor then updates the broker concerning the base station list. In the meantime, the broker delegates all service calls to the temporary buffer base station until it is notified about the construction of a survivable base station. After building the secure and survivable base station, the factory deploys the new base station, and the buffer base station is revoked from service. Again, the monitor is informed about the creation of the secure and survivable base station, which in turn informs the broker about the deployment of a new base station. To make the service more robust, the factory can generate multiple copies of the secure and survivable base station for possible use in the future.

Although this approach supports the service availability to the user and cluster head continuously, the new base station might still be susceptible to the same failures or attacks. In order to connect to the new base station, the user and cluster heads need to stub of the new base station. This can hide the location of the base station from the attacker using different binding information. Although the attacker figures out the new location of the base station, it cannot send any messages to the base station, because the communication port number of the base station and even the interfaces has been changed.

5.1. Key Management Scheme

A key management procedure is an essential constituent of network security. Symmetric key systems require key to be protected. Insecure environments like those sensor networks will be used in make this even more important. Moreover, sensor networks have energy and computational constraints. Therefore it is necessary to maintain a balanced security. We propose a key management scheme for sensor networks, with the objective of minimizing the computation, communications and storage overhead by key management.

In our approach the nodes use a symmetric key mechanism; therefore each node should store the keys if shares with it's the higher levels of the network hierarchy. Since the sensors are memory constrained and are susceptible to attacks by the adversary, they should be assigned the minimum number of keys. Assigning minimum number of keys saves memory. In case a node is compromised it also helps to reduce the impact of the damage since less number of keys would be revealed to the adversary. As soon as the sensor nodes are deployed, all the sensor nodes and clusters send their ID to the base station. In our key management scheme consists of three keys:

- K_g (group key) - Generated by base station, pre-deployed to all sensor nodes in the entire network. Node uses this key to encrypt the data.
- K_{cl} (cluster key) - Generated by base station to all the cluster heads in the entire network. Base station and nodes from the cluster head use this key to decrypt the data.
- K_s (sensor key) - Generated by the base station to all the sensors in the entire network. The base station use this key to encrypt the data to send to the cluster head.

In our key management schemes, when base station sends a message to the cluster head, it constructs the message as follows:

$\{ K_g, K_{cl}, MAC, ID, TS, N, Message \}$

Base station encrypts its own ID and a current time stamp TS. Base station generates a random number N and K_{cl} for cluster header. Cluster head checks the ID from the packet, if the ID in the packet matches the ID its holds, verifies the authentication and integrity of the packet through MAC. Otherwise, packet is dropped by the cluster head. The base station builds the message using the fields below:

EK_s { K_g, K_{cl}, MAC, ID , TS, N , Message }

Base station encrypt the message and broadcast the data. When the cluster head receives the messages, it decrypts it by using K_s. Cluster head aggregates the messages received from its nodes and forwards it to the next level cluster head or if the cluster head is one hop closer to sensor node. Receiving cluster head checks its routing table and constructs the following packets to be sent to the next level cluster head. The cluster head adds it own ID and rebuild the packet as the following:

{ ID_{cl}, { K_g, K_{cl} , MAC, ID_{cl}, TS , N , Message }

Here the ID is the ID of the receiving cluster head which wraps the message and sends to the next hop cluster head or to the lowest cluster head. Next hop cluster head receives the packet and checks its own ID, if the ID in the packet is the same as its holds, it updates the ID for the next hop and broadcast it, or else the packet is discarded. Aggregate message refers to the message aggregated by the cluster head. Finally, all the cluster head receives Kcl and Kg generated by the base station. When cluster head sends the message to the sensor nodes, it constructs the messages as follows:

{ ID_{cl}, K_g , TS , MAC, N , Message }

Finally, the sensor node gets K_g for use to encrypt the message in order to send to the cluster head. In our key management schemes all the key are generated by the base station. Base station also verify MAC and data and also process aggregate data. Cluster head aggregate data coming from the sensor nodes and then send to the base station. In our scheme, we use message authentication code (MAC). It is efficient symmetric cryptographic primitive for two party authentication. For any message, a secure MAC function prevents on attacker without prior knowledge of the secret key from computing the correct MAC. A MAC achieves authenticity for point-to-point communications because a receiver knows that a message with the correct MAC must have been generated either itself or by the sender. The sequence diagram of key management scheme is as shown in figure 4.

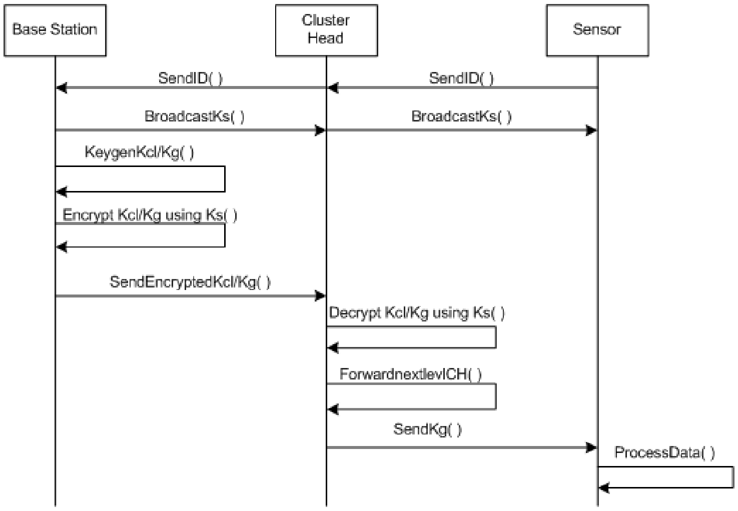

Figure 4. Sequence Diagram of Key Management Scheme

Our key management scheme convenient for resource constraints sensor network. Because we use symmetric key management scheme, it reduces computational overhead and saving energy consumption. Moreover, our scheme gives robust to packets loss and short authentication latency and low communication overhead and only need low storage requirements in memory. Identically, the scheme that recovers from any loss of packets, has no authentication latency, can individually authenticate packets, has negligible overhead, and has a computation cost similar to what is found in symmetric cryptographic primitives. This key management scheme also gives strong encryption and authentication among sensor nodes to protect confidentiality, integrity and availability of the communications and computation of wireless sensor network. This encryption increase the resistance of the WSNs. Resistance refers to the capability of a system to deter attacks and is one of the survivability requirements services.

6. Conclusions

In this paper, we have outlined some important security requirements and survivability requirements for WSNs. Based on the study about the security requirements and survivability requirements, we have developed architecture and proposed a framework for secure and survivable WSNs. Sensor networks are often organized hierarchically, with a base station which is responsible for data collection and management of a wireless sensor network (WSN). The base station is a single point of failure and if attacked it can bring down the entire wireless sensor network. This paper concerns strategies for increasing survivability of WSN against a variety of threats that can lead to the failure of the base station. We use key management scheme as a case study to better understanding of the interaction between security and survivability. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security and survivability will be required of these WSN applications. This will be our future research.

References

1. *I. Akyildiz, W. Su, Y. Sankarasubramanian, and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazines, August 2002, vol. 40, no. 8, pp. 102-114.*
2. *M. Saraogi, "Security in Wireless Sensor Networks", Project Paper, 2003.*
3. *M. Sharifnejad, M. Sharifi, M. Ghiasabadi, S. Beheshti, "A Survey on Wireless Sensor Networks Security," 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (SEIT), TUNISIA, March 2007.*
4. *T. Zia, A. Zomaya, "A Security Framework for Wireless Sensor Networks," IEEE Sensors Applications Symposium Houston, Texas USA, February 2006.*
5. *T. Zia, A. Zomaya, "A Secure Triple-Key Management Scheme for Wireless Sensor Networks," Proceedings of 25th IEEE International Conference on Computer Communications (INFOCOM 2006) April 2005, PP. 1-2.*
6. *Y. Qian, K. Lu, D. Tipper, "Towards Survivable and Secure Wireless Sensor Networks," Performance, Computing, and Communications Conference, (IPCCC 2007) IEEE International, Volume , Issue , April 2007, PP. 442-448.*
7. *Y. Qian, K. Lu, B. Rong, H. Zhu, "Optimal Key Management for Secure and Survivable Heterogeneous Wireless Sensor Networks," Global Telecommunications Conference, 2007. GLOBECOM 07. IEEE, Nov 2007, PP. 996 - 1000.*
8. *X. Li, D Yang, "A Quantitative Survivability Evaluation Model for Wireless Sensor Networks," Proceedings of the IEEE International Conference on Networking, Sensing and Control, ICNSC 2006 , PP. 727 - 732*
9. *B. Ellison, D. A. Fisher, R.C. Linger, H. F. Lipson, T. Longstaff , N. R. Mead, "Survivable Network System: An Emerging Discipline," Technical Report CMU/SEI-97-TR-013, Software Engineering Institute, Carnegie Mellon University, Tech. Rep., 1999*
10. *J.P. Walters, Z. Liang, W. Shi, V. Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC press.*