A Survey on Security Solutions in Wireless Sensor Networks

Hind Annahidh
433203143@student.ksu.edu.sa

Soha S. Zaghloul
smekki@ksu.edu.sa

College of Computer and Information Science
Department of Computer Sciences
Kind Saud University
Riyadh, Saudi Arabia

ABSTRACT

Wireless Sensor Networks are deployed in sensitive and unattended areas that cannot be reached by human beings. Therefore, it is difficult to maintain them. In addition, sensors are of limited memory, processing power and energy by nature. By consequence, this makes WSN subject to attacks such as network failure, data acquisition and modification, etc. Many security solutions are exposed in the literature to overcome this problem. Secure data aggregation, encryption and authentication, and key management are developed to maintain the security of the WSN. This paper overviews different security solutions in the literature and illustrates their target. Moreover, it conducts a comparative study between them in terms of confidentiality, integrity, freshness and authentication.

KEYWORDS

Wireless Sensor Networks; Secure Data Aggregation; Encryption; Authentication; Key Management.

1 INTRODUCTION

A wireless sensor network (WSN) consists of a number of sensor nodes which are dispersed geographically. A sensor is characterized by its small size and low cost. In addition, it is limited in its memory capacity as well as its power energy. Its role is to sense the environment which is deployed in through a specific hardware.

Sensor nodes are deployed in harsh and sensitive areas that cannot be attended by human beings. Examples include military sensing and tracking missions, disaster management, environment monitoring, and patient monitoring.

WSNs gain their value from their low cost and useful applications. On the other hand, WSNs are prone to attacks since they are deployed in unmonitored environments. Traditional security solutions cannot be applied in WNS due to sensors' constraints and the limitation in its resources which lies in low power or restricted energy.

This paper surveys the deployed WSN security solutions. Section 2 overviews the security issues encountered in WSN. Section 3 discusses the data aggregation protocols. Section 4 exposes two protocols of cryptography and authentication protocols. Section 5 presents key management protocols. Finally, section 6 concludes the paper.

2 SECURITY ISSUES

WSN are vulnerable to attacks due to the broadcast nature of the transmission medium. On the other hand, sensors are cultivated in harsh environment unattended by human beings. Therefore, they are physically unprotected. In this section, basic security issues are exposed [1].

2.1 Attack and Attacker

An attack is defined to be an effort to get illegal access to a service, information or to affect the integrity, confidentiality or availability of a system.

WSN attackers are divided into categories. Here they are:

Passive versus active: a passive person or entity is that who only eavesdrops or monitors the communication channel. On the other hand, an active person or entity exerts more malicious effort such as adding, deleting or modifying the transmitted information on the channel.

Outsider versus insider: outsider attacks are performed by the nodes that do not belong to the network. On the other hand, insider attacks are nodes inside the network in concern that behave in unauthorized ways.

Mote-class versus laptop-class attacks: in mote-class attacks, view nodes of similar capability to the network nodes in concern are used to attack the WSN. On the other hand, laptop-class uses more powerful devices than those deployed in the network in concern to attack the WSN. These powerful devices are characterized by their great processing power, transmission range and battery power. Examples of such devices include laptops.

2.2 Security Requirements

The goal of the security is to protect the network against attacks. These may affect the information and/or the resources in the network. In order to have a secure system, the following criteria are investigated [1]:

- *Authentication*: ensures that the data are initiated from the exact resource.
- *Confidentiality*: ensures that only authorized nodes can get the messages.
- *Integrity*: ensures that any received message is not modified by any unauthorized parties.
- *Freshness*: ensures that the data are recent; it also guarantees that the attacker does not replay to old messages.

3 SECURE DATA AGGREGATION

The aim of secure data aggregation is to control traffic in the WSN. This is performed by providing an additional function to some nodes in the network; namely, the accumulation of the data from other nodes, and their transfer to the base station. Such protocol is useful in networks that suffer from traffic because of the large number of nodes.

Arranging the sensor nodes of a network in a tree structure, then only the root transmits data to the base station to which it is directly connected. The leaves act as normal nodes. The rest of the nodes at the remaining levels of the tree take the information from the children, sum it with its own data, and transfer it to the direct parent node. Figure 1 illustrates such function.

In Figure 1, the WSN consists of 18 nodes. They use the sum function to minimize the energy consumption by reducing the number of bits received by the Base Station. The nodes in yellow (N10 to N18) are normal nodes that do not perform any aggregation function. The green nodes (N2 to N9) conduct additional processing by summing their values to those of their children and transfer the result to the corresponding parents. For example, if the reading values of N5, N10 and N11 are 6, 3 and 5 respectively, then the aggregate value at N5, the parent node, is the sum of these values which 14. Assuming that the reading values at N2 is 2, and that the aggregated value at N6 is 10, then the aggregating value at N2 is 2+14+10=26, and so on.

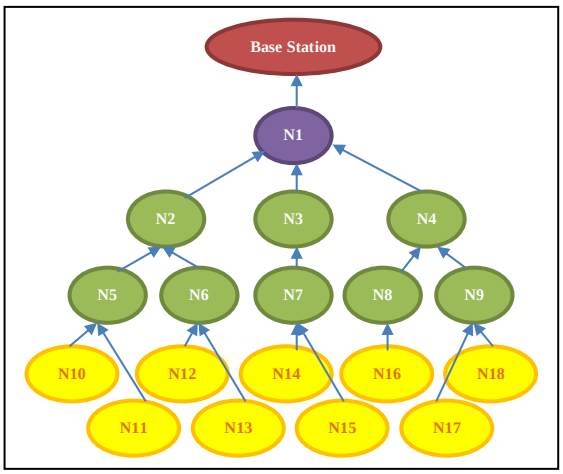

Figure 1: Secure Data Aggregation

Obviously, this reduces the number of transmissions in the network. Without aggregation, the 18 nodes would compete to send to the base station. However, only N1 sends to the base station with the data aggregation protocol. Alleviating traffic decreases the probability of the occurrence of bottlenecks in the networks. Therefore, network failures are less likely to occur.

Data aggregation models are classified into two types. First, the one-aggregator model, in which only one node plays the role of an aggregator. This is usually deployed in networks with relatively small number of sensor nodes. The second model is

the multiple-aggregator model, in which multiple nodes are provided with the aggregation capability function. This is usually used in networks with large number of nodes. The model illustrated in Figure 1 is the multiple-aggregator mode.

On the other hand, the secure data aggregation model suffers from some disadvantages. The most important of which is that it is vulnerable to attacks since information might easily be captured and inadvertently modified at the aggregator nodes. Consequently, many schemas were proposed to overcome this severe problem. These are secure data aggregation (SDA), secure information aggregation (SIA), witness based data aggregation (WDA), SecureDAV, secure hop-by hop data aggregation protocol (SDAP), Secure Reference-Based Data Aggregation scheme (SRDA). They differ in terms of their degree of meeting the network security requirements.

3.1 Comparing Data Aggregation Schemes

Table 1 summarizes the characteristics of the previously mentioned data aggregations schemes. A scheme is selected based on many factors such as the network needs, data aggregation model (one-aggregator or multiple-aggregator), the number of nodes and the adversary type [2]. In Table 1, 'C' stands for data confidentiality, 'F' designates data freshness, 'I' stands for data integrity, whereas 'A' stands for authentication.

4CRYPTOGRAPHY AND AUTHENTICATION

The aim of cryptography is to ensure that the data are kept protected. Authentication guarantees that the data are accessed by authorized persons only. In this section two encryption and authentication protocols are presented [3].

4.1 SPINS

Sensor Protocols for Information via Negotiations (SPINS) is a routing protocol built on the top of the operating system TinyOS. SPINS consists of two building blocks; namely, SNEP and µTESLA.

Secure Network Encryption Protocol (SNEP) provides data confidentiality. In addition, it protects data authentication between two parties. Furthermore, it ensures data integrity, replay protection and data freshness. The most important advantage of SNEP is that it imposes a very low overhead communication; thus making it compatible with sensor limited capabilities [4][5].

On the other side, µTESLA is the micro version of TESLA, the Timed Efficient Stream Loss-tolerant Authentication. It provides authenticated broadcast. SPIN security characteristics are summarized in Table 1.

Table 1. Comparing Data Aggregation Schemes

SCHEME	C	F	I	A
SDA	N	Y	Y	Y
SIA	Y	Y	Y	Y
SHDA	N	Y	Y	Y
WDA	N	Y	N	Y
SDAP	Y	Y	Y	Y
SECUREDAV	Y	Y	N	Y
ESA	Y	Y	Y	Y

4.2 TinySec

This is a lightweight generic security package. The most important characteristic of TinySec is its flexibility since it can be easily integrated into WSN applications.

TinySec is a data link layer security protocol. It provides authentication and message integrity. In addition, it ensures data confidentiality and replay protection.

TinySec provides two security options: authenticated encryption (TinySec-AE) and authentication only (TinySec-auth). Table 2 shows TinySec security characteristics [6].

Table 2. Comparing Encryption and Authentication Protocols

Protocol/ Scheme	C	F	I	A
SPIN	Y	Y	Y	Y
TINYSEC	Y	N	Y	Y

5 KEY MANAGEMENT

Encryption is achieved by defining a key between communicating nodes. Many protocols perform key creation, establishment and management. The selection of a protocol as a key manager depends on the properties of the protocol and their adaptability

to the application requirements. In this section, applications' requirements are represented. In addition, key management protocols are exposed with their corresponding properties [7].

Application requirements are summarized in the following points:

- *Memory Footprint (Mm):* this is defined as the space of memory (ROM and RAM) allocated by the protocol.
- *Communication Overhead (Cm):* this is defined as the number of messages exchanged between peers.
- *Processing Speed (Sp):* this is defined as the computational cost of the protocol.
- *Network Bootstrapping (sec):* this is the confidentiality of the bootstrap process.
- *Network Resilience (Rs):* this is the resistance against stolen credentials.
- *Connectivity (GC):* this is the existence of a key path between any two nodes.
- *Scalability (SC):* this is the support for big networks.
- *Extensibility (Ex):* this is the capability of adding new nodes.
- *Energy (En):* this is the optimization of the energy usage.

5.1 LEAP

Localized Encryption and Authentication Protocol (LEAP) is a key management protocol. It establishes four types of keys which are individual keys, pairwise shared keys, cluster keys and group keys.

Individual keys are symmetric keys shared between the base station and each of the nodes. On the other hand, pairwise shared keys are symmetric keys shared between a node and each of its neighbors. However, neighbors do not share the key with each other. Cluster keys are symmetric keys shared between a node and all of its neighbors. The group key, a symmetric key shared with all nodes of the network and the base station [4].

LEAP provides authentication and confidentiality in a wireless environment. Table 3 shows LEAP security characteristics.

Table 3: LEAP Characteristics

Protocol/ Scheme	C	F	I	A
LEAP	Y	N	N	Y

5.2 Other Key Management Protocols

Key Infection, EDDK, and Public Key Cryptography-Based (PKCB) are three well-known key management protocols. Table 4 summarizes the advantages and drawbacks of each of them.

Table 4. Properties of Key Management Protocols

	Key Infection	**EDDK**	**PKCB**
Cm	-	+	++
GC	++	++	++
Lc	++	++	++
NC	--	+	++
En	+	--	-
Ex	--	++	++
Mm	++	--	+
Rs	++	++	++
Sc	++	++	++
Sec	--	+	+
Sp	+	--	--
NOTATION			
(++)	Advantage		
(--)	Disadvantage		
(+)	Advantage depending on the protocol design		
(-)	Disadvantage depending on the protocol design		

6 CONCLUSION

WSN are deployed in harsh and unattended environment. Consequently, this makes it difficult to protect and maintain its security. Sensor nodes are therefore vulnerable to attacks. Security protocols should therefore be developed for WSN taking into consideration the natural constraints of the sensors. Solutions should consume as least as possible of the processing power of the nodes. In addition, they should occupy the least amount of sensors' memory.

Many solutions are exposed in the literature. This paper presents three main security solutions used for different purposes. The secure data aggregation

is deployed to control the traffic in WSN. On the other hand, SPINS and TinySec are selected to provide data encryption and authentication. Finally, LEAP is the solution for key management.

This research overviews the security solutions in the literature. It sheds light on three main solutions. Moreover, it conducts a comparative study between them.

7 REFERENCES

1. Modares, H., Salleh, R., Moravejosharieh, A.: Overview of Security Issues in Wireless Sensor Networks. In 3rd International Conference on Computational Intelligence, Modelling and Simulation, 2011.
2. Sang, Y., Shen, H., Inoguchi, Y., Tan, Y., Xiong, N.: Secure Data Aggregation in Wireless Sensor Networks: A Survey. In IEEE 7th International Conference on Parallel and Distributed Computing, Applications, and Technologies (PDACT'06), 2006.
3. Kim, T., Kim, C., Hong, C., Kim, H.: Comparison of Security Protocols for Wireless Sensor Networks. www.academia.edu.
4. Sangwan, A., Sindhu, D., Singh, K.: A Review of Various Security Protocols in Wireless Sensor Networks, 2011.
5. Ahmed, A.: An Evaluation of Security Protocols on Wireless Sensor Networks. Seminar on Internetworking, 2009. http://www.cse.tkk.fi/en/publications/B/5/papers/ahmed_final1.pdf.
6. Sharma, K., Ghose, M., Kumar, D.: A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks. International Journal of Advanced Science and Technology, 2010.
7. Alcaraz, C., Lopez, J., Roman, R., Chen, H.: Selecting Key Management Schemes for WSN Applications. Journal of Computers and Securiy, 2012.