ICIC Express Letters
Part B: Applications
Volume **11**, Number **11**, November **2020**

 ISSN 2185-2766
pp. **1087–1093**

ANALYSIS OF SECURITY PROTOCOLS IN WIRELESS SENSOR NETWORKS

Seongwook Youn

Department of Software
Korea National University of Transportation
Daehak-ro 50, Chungju-si, Chungcheongbuk-do 27469, Korea
youn@ut.ac.kr

Received March 2020; accepted June 2020

Abstract. *Nowadays, Wireless Sensor Networks (WSNs) are being used in area monitoring, health care monitoring, environmental/earth sensing, industrial monitoring, and therefore security of these networks is becoming a major concern. WSN consists of low power, low-cost smart devices that have limited computing resources against current devices, like personal computer. This paper discusses overall constraints, security requirements, security threats, typical attacks and their defensive techniques or countermeasures relevant to the sensor networks. Also, several security protocols in sensor network environment are compared.*
Keywords: WSN, Sensor, Security, Protocol

1. **Introduction.** WSNs are a collection of many sensor nodes that are self-organized and are capable of wireless communication. However, these nodes are constrained in terms of size, memory, energy, processing power. All nodes communicate to each other over short distances and perform limited processing. Sensor nodes send and receive data containing command to control special tools or hardware, during the communication. Because of this, providing information security during the communication is one of the main jobs. Security challenges of sensor networks are different from traditional networks due to many constraints of these networks [1]. This research aims to give an understanding of a security protocol in WSN and contributes that security protocol developers in WSN must consider energy consumption together.

1.1. **WSN constraints.**

Resource constraints: Sensor nodes contain limited resources like small memory (typically 4 KB of RAM), restricted computational capability (about 4-8 MHz) and small power source (battery power, e.g., ReVibe Energy, Perpetuum).

Local addressing schemes: Because nodes are large in numbers, it is impossible to implement a global addressing scheme.

Message size is small: Data size that is sent by nodes is small compared with existing networks.

Security constraints: Many security algorithms that are used in existing networks, namely, cryptographic algorithms, are not suitable in WSN because of resource constraints. Besides that, sensor networks operate in hostile environment.

1.2. **Security requirements.** Availability, confidentiality, integrity, authenticity and non-repudiation were considered as security services that should be provided by sensor networks [1].

Availability is to ensure that the network is able to provide services at any time for the authorized users. Various mechanisms are used to save energy and extend the life

DOI: 10.24507/icicelb.11.11.1087

of network, but also to prevent Denial of Service (DoS). Confidentiality is to ensure the secrecy of the data transmitted between sensor nodes by limiting the data access to intended users only. It is mainly based on the use of cryptographic techniques at physical layer, where data is encrypted at the sending node to prevent information disclosure to unauthorized users. Integrity is to assure that the data transmitted cannot be altered during transmission until it reaches its original destination. The data integrity may be breached by having a malicious node in the network. Authenticity is to ensure the identity of sender must always be verified so that no intruder may be able to forge wrong data into the network. Non-Repudiation is to ensure neither the sender nor the receiver should be able to deny that the message is sent by him.

Besides that, the additional security requirements for WSN have to be defined in [2]. These requirements can be grouped as follows.

1.2.1. *Data level requirements.*

a) Anonymity is providing information protection and confidentiality by hiding the source of the data.
b) Freshness is to ensure that data is not duplicated and is recent.

1.2.2. *Access level requirements.*

a) Authentication is to ensure that received message comes from true sources.
b) Authorization is to ensure that only authorized users or devices have the access to the network.
c) Accessibility is to ensure that sensor nodes have the access to the authorized information only.

1.2.3. *Network level requirements.*

a) Robustness/Resiliency is to guarantee that the network is able to function and serve the purpose if the number of nodes increases or in the case of some nodes being compromised.
b) Self-organization is having the sensor nodes that are independent and fiexible to self-organize in the case of any node failure or new nodes joining the network.
c) Time synchronization can be required for different purposes, such as the power conservation, computation of the packet's end-to-end delay, and the group synchronization for tracking applications.

2. **Related Works.** There are several articles on the security protocols used in the WSN network. Some of them are dedicated to the energy consumption of the protocols, while others are devoted to the security of protocols. Authors discuss typical constraints, security goals, threat models and typical attacks on sensor networks and their defensive techniques or countermeasures relevant to the sensor networks, including security methods [3]. In addition, energy consumption of security algorithms, and cryptographic algorithms used in security protocols are not enough discussed. Tanveer and Zomaya [4] documented security issues in wireless sensor networks and countermeasures against the threats posed by these issues. The paper is a good example of security problems in WSN. Besides that, Guo et al. created Petri Net model to prove the security of the security protocols, such as, SNEP, and iTESLA [5]. However, the analysis of security protocols, the analysis of the widely used security protocols on energy consumption and security levels have not been fully analyzed. Fazlic et al. discussed various vulnerabilities and security threads in differenct applications of WSN in the real world, such as intrusion, black hole attack, and selective forwarding attack. Finally, they proposed protocols for secure transfer of data [6]. Their research explained many examples of attack.

3. Security Threats and Issues in Wireless Sensor Networks.

3.1. Threat models.

Threats in wireless sensor network were classified by Karlof and Wagner [7] as the following:

a) Outsider versus insider attacks: The outsider attacks are made from nodes which do not belong to a WSN. External attacker has no access to most cryptographic materials in WSN. The insider attacks are made from nodes that are in WSN. The inside attacker may have partial key material and the trust of other sensor nodes. Inside attacks are much harder to detect.
b) Passive versus active attacks: A passive attack is a sensor network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. An active attack is a sensor network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.
c) Mote-class versus laptop-class attacks: In mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities as that of network nodes. In laptop-class attacks, an adversary can use more powerful devices like laptop, and can do much more harm to a network than a malicious sensor node.

3.2. Attacks in wireless sensor networks.

Attacks on WSNs can be divided into two categories [8]: attacks against the security mechanisms and attacks against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks.

3.2.1. *Denial of Service.* Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. A Denial of Service attack is an attempt to make a computer system (server or client) or some other resource unavailable to legitimate users. Normally, this attack is considered to be a problem of computer network, but for a single CPU also it can be present among various resources. The motive or target of a DoS may vary from person to person but in general, it aims to prevent some services from functioning efficiently either temporarily or indefinitely.

There are so many types of DoS attacks. Each layer is vulnerable to different kinds of DoS attack and has different options for its defense. Classification of Denial of Service attacks is given in [9]. At physical layer it could be in the form of Jamming and Tempering attack, at the data link layer the attack could be Interrogation, Denial of Sleep, Collision, Exhaustion and Unfairness, at the network layer DoS attack could be IP Spoofing, Replaying, Homing, Altering Routing Tables, Black Hole, Neglect and Greed, Sinkhole, Sybil, Wormhole, Acknowledgement Spoofing, Hello flood attack, and at the transport layer this attack could be SYN flood, Desynchronization, and at the application layer DoS attack could be overwhelming sensors, Path based routing, Deluge (reprogramming).

3.2.2. *Attacks on information during transmission.* The most dangerous attack in WSN is on information that is being transmitted between nodes because that information is susceptible to eavesdropping, injection, modification. Traffic analysis attack can also be performed because attacker may be able to get to know about the layout of the network and can damage the busiest portions of the network to perform greatest damage.

3.2.3. *Replicating a node attack.* The attacker may insert a new node into the sensor network, which can be a clone to a preexisting node. This new cloned node can transmit useful information to the attacker. This node replication attack is the most dangerous when the cloned node is some base station. Therefore, base stations need to be deployed in secure locations.

4. **Security Protocols in Sensor Networks.** Traditional security solutions cannot be applied to wireless sensor network because these are resource-constrained networks. Therefore, a lot of research is going on to develop security protocols for these resource-constrained networks. Most security protocols that exist today require a lot of computation for which large memory is required which is a major constraint of this network. Therefore, we present the analysis of existing security protocols in this section.

4.1. **SPINS: Security protocols for sensor networks.** This protocol was proposed by Perrig et al. and it consists of two secure building blocks: SNEP and μTESLA [10]. SNEP includes data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments.

4.1.1. *SNEP: Sensor network encryption protocol.* This sub-protocol provides data confidentiality, authentication, integrity and message freshness. Confidentiality and message freshness are performed by using block cipher in counter mode. Data integrity and authentication are done with message authentication code in counter mode. Besides that, this protocol has low communication overhead since it only adds 8 bytes per message.

4.1.2. *μTESLA: Authenticated broadcast.* Current proposed authentication methods are impractical for WSN due to relying on public key based digital signatures schemes. Digital signature based authentication requires long signatures with high communication overhead of 50-1000 bytes per packet, very high overhead to create and verify the signature. μTESLA is based on TESLA that has an overhead of approximately 24 bytes per packet and based on digital signature. In μTESLA protocol a node stores the packet in the buffer till the key is disclosed. The time when the key is disclosed, the base-station broadcasts verification key to all the receivers, which the node can use to authenticate the packet stored in its buffer. One way function F (I just used "one way function" as a function hard to invert given input.) is used to disclose keys from last key K_n by $K_i = F(K_{i+1})$. Authentication is performed by MAC that is easier than public key based digital signature.

4.2. **TinySec.** This protocol was designed by Karlof and Wagner [7] and provides authentication, message integrity and confidentiality. Replay protection was not addressed by TinySec. Authors believe higher layer protocols should handle this. This protocol was used in two modes: TinySec-Auth and TinySec-AE. The first only provides message authentication and integrity. The second one is used to add encryption to TinySec-Auth. Message authentication and integrity are performed by using MAC. Stream ciphers and block cipher in CBC mode can use to provide message confidentiality [11].

4.3. **Zigbee.** Zigbee defines new higher layer communication protocol based on IEEE 802.15.4 standards [12]. This protocol has high level security but low level power saving. Zigbee network consists of three types of network devices – the Zigbee Coordinator, Zigbee Router and Zigbee End Device. Zigbee Coordinator starts network communication, stores information in the network and bridges the various networks. Zigbee Router helps in linking various devices with each other and provides multi-hop communication. Zigbee End Device is composed of Sensors, Actuators and Controllers that collects data and communicates with other Zigbee components. This protocol provides authentication by trust manager role, replay protection, message integrity and confidentiality by configuration manager role. Zigbee operates in both Residential Mode and Commercial Mode that has low security and high security respectively [3].

4.4. **MiniSec.** This protocol works network layer and has lower energy consumption than TinySec but level of security matches with that of Zigbee [13]. This protocol has two operating modes: one tailored for single-source communication, and the other tailored for multi-source broadcast communication. It uses Offset Codebook Mode (OCB) as its block cipher mode of operation. MiniSec provides message authentication, replay protection, confidentiality, integrity. Message confidentiality and authentication are provided by block cipher – Skipjack in OCB mode.

4.5. **LEAP: Localized encryption and authentication protocol.** Key management protocol for sensor networks called LEAP was proposed by Zhu et al. [14]. It provides authentication and confidentiality. In addition to it, LEAP has following features.

- LEAP provides four types of keys for each sensor node – an individual key shared with the base station, a pairwise key shared with other sensor nodes, a clustered key shared with multiple neighboring nodes, and a group key shared by all nodes in the network.
- LEAP includes use of one-way key chains for local broadcast authentication.
- A distinguishing feature of LEAP is that its key sharing approach supports in-network processing, while restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node.

4.6. **Others.** There are many security protocols for WSNs. Some of them provide all security requirements like above description and some of them only provide one security feature. For example, fingerprint-based user authentication protocol with one-time password is proposed by Liu et al. [15] and ticket-based authentication protocol for underwater WSNs is proposed by Yun et al. [16]. Besides that, SPIN protocol is improved by Dutta et al. using TOSSIM operation system [17]. Following table (Table 1) shows

Table 1. Comparative analysis of existing protocols for WSNs

Protocols	Authentication	Integrity	Confidentiality	Replay protection	Attacks deterred
SPINS	MAC based	MAC based	Block ciphers, DES-CBC	Yes, by counter	Data and information spoofing, message replay attacks
LEAP	MAC based	MAC based	Block ciphers, RC5 in CBC	No	Data and information spoofing
TinySec	MAC based	MAC based	Block ciphers in CBC mode, stream cipher	No	Data and information spoofing
MiniSec	MAC based	MAC based	Skipjack or RC5 in OCB mode	Yes, by counter	Data and information spoofing, message replay attacks
Zigbee	MAC based	MAC based	AES-128 in CCM mode	Yes, by counter	Data and information spoofing, message replay attacks

the comparison of these security protocols on the basis of some features like encryption, and freshness. Furthermore, security and energy consumption analysis of SPINS, Zigbee, MiniSec, LEAP and TinySec is described in Figure 1 [1]. Based on comparison analysis, the most important two aspects of WSN protocols are security and energy consumption. Hence, protocol should be designed by considering security and energy consumption.

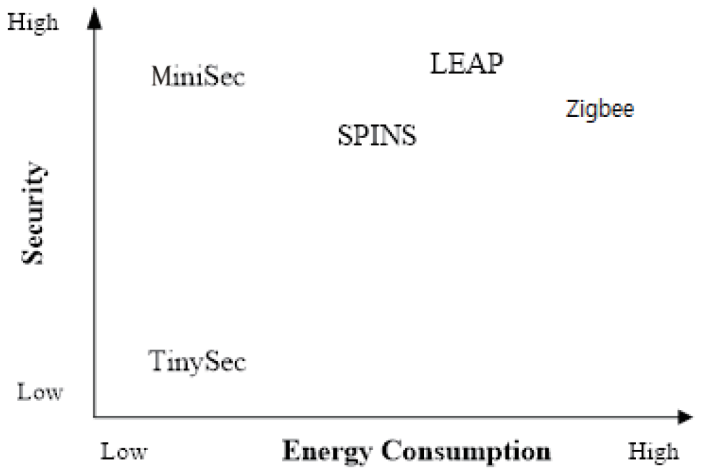

FIGURE 1. Security and energy consumption analysis of protocols for WSNs [1]

Also, several existing protocols for WSNs are compared in the aspect of authentication, integrity, confidentiality, replay protection and attacks deterred.

5. **Conclusion and Future Scope.** A comparative analysis has been made based on the characteristics of each security protocol. As a result of the analysis, it was found that the security protocols contained the message authentication, integrity and confidentiality on the basis of symmetric algorithms requiring small energy consumption. Additionally, in some protocols, counters (SPINS, MiniSec, Zigbee) have been used to against the replay attacks. To develop a new protocol is resistant to attacks on WSN, which provides low energy consumption and message authentication, integrity and confidentiality. In the future, a research on constraints of sensor node itself and security issues against WSN and IoT environment should be done together.

REFERENCES

[1] B. Monika, N. Pandey and B. Kumar, Security protocols for wireless sensor networks, *IEEE International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015.
[2] T. Ivana and J. A. McCann, A survey of potential security issues in existing wireless sensor network protocols, *IEEE Internet of Things Journal*, vol.4, no.6, pp.1910-1923, 2017.
[3] S. Ritu, Y. Chaba and Y. Singh, Analysis of security protocols in wireless sensor network, *International Journal of Advanced Networking and Applications*, vol.2, no.3, pp.707-713, 2010.
[4] Z. Tanveer and A. Zomaya, Security issues in wireless sensor networks, *International Conference on Systems and Networks Communication*, 2006.
[5] Y. Guo, X. Liu and X. Shao, Formal proof of the security protocol in wireless sensor network based on the Petri Net, *The 9th International Conference on Computational Intelligence and Security (CIS)*, 2013.
[6] F. Fazlic, S. A. Hashemi, A. Aletic, A. A. almisreb, S. M. Norzeli and N. M. Din, A survey on security in wireless sensor network, *Southeast Europe Journal of Soft Computing*, 2019.
[7] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, *Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 2003.
[8] P. A. Khan, H. Lee and C. S. Hong, Security in wireless sensor networks: Issues and challenges, *The 8th IEEE International Conference Advanced Communication Technology (ICACT)*, 2006.

[9] D. Buch and J. Devesh, Denial of Service attacks in wireless sensor networks, *International Conference on Current Trends in Technology*, 2010.

[10] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen and D. Culler, SPINS: Security protocols for sensor networks, *Wireless Networks*, pp.521-534, 2002.

[11] K. Chris, N. Sastry and D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, *The 2nd ACM International Conference on Embedded Networked Sensor Systems*, 2004.

[12] ZigBee Specification, *v1.0: ZigBee Specification*, San Ramon, CA, USA, 2005.

[13] M. Luk, G. Mezzour, A. Perrig and V. Gligor, MiniSec: A secure sensor network communication architecture, *The 6th IEEE International Symposium on Information Processing in Sensor Networks (IPSN)*, 2007.

[14] S. Zhu, S. Setia and S. Jajodia, LEAP+: Efficient security mechanisms for large-scale distributed sensor networks, *ACM Trans. Sensor Networks (TOSN)*, vol.2, no.4, pp.500-528, 2006.

[15] X. Liu, Y. Shen, S. Li and F. Chen, A fingerprint-based user authentication protocol with one-time password for wireless sensor networks, *IEEE International Conference on Sensor Network Security Technology and Privacy Communication System (SNS&PCS)*, 2013.

[16] C. Yun, J. Lee, O. Yi and S. Park, Ticket-based authentication protocol for underwater wireless sensor network, *The 8th IEEE International Conference on Ubiquitous and Future Networks (ICUFN)*, 2016.

[17] R. Dutta, S. Gupta and D. Paul, Energy efficient modified SPIN protocol with high security in wireless sensor networks using TOSSIM, *International Conference on Parallel, Distributed and Grid Computing*, 2014.