A Survey of Security Protocols for Wireless Sensor Networks

John Gichuki Ndia

Department of Information Technology,

Murang'a University of Technology, Murang'a-Kenya

ndiajg@gmail.com; ndia.john@mut.ac.ke

Abstract

There are numerous wireless sensor network (WSN) applications being developed day to day. These applications range from simple environmental monitoring such as collecting temperatures in an agricultural farm to complex applications such as monitoring battle fields. As the applications increase so are the attacks. Therefore, several security protocols have been introduced to be used with the different applications which have varying security requirements; this implies that the choice for the WSNs application should be well considered. This paper discusses the wireless sensor network security requirements, the most common attacks and the most popular protocols used with WSNs. Focus is also given to the strengths and limitations of WSN security protocols to enable designers of the WSNs choose the right protocol for their applications.

Keywords: WSNs, Security protocol, Security requirement, WSN attacks

1. Introduction

A wireless sensor network (WSNs) comprises of many identical nodes with limited resources. Sensor nodes communicate wirelessly and they intelligently process signals and transmit data over the networks. These nodes are normally spread over the whole network area for monitoring, data collection, processing, and forwarding to a base station to process further (Sharma, Chaba & Singh, 2010).

The Sensors are small in size, limited in terms of power and their cost is normally low. Sensors have the following capabilities: communication is over short distances, they can sense or read data from the environment, and their data processing capability is limited. Normally sensor operates at 2.4 GHz frequency, 250Kbps data rate, flash memory is 128KB, memory of 512KB for purpose of recording measurements, they transmit powers ranging from 100uW and 1mW, and communication range is between 30m to 100m. Therefore, the greatest design consideration should be energy efficiency of WSN protocols (Uluagac et al., 2008).

The greatest challenge for WSNs are security issues, and for certain sensor networks applications, like health care applications and military applications security becomes even more crucial. These challenges are as follows;

i. It's difficult to protect wireless communication since it is done by broadcasting. Packets can be injected, eavesdropping is a possibility, interception of moving data, and data transmitted can be altered easily by adversaries.

ii. The WSNs may be installed in environments that are potentially insecure; where there is a possibility for adversaries to masquerade as authorized nodes in the network, and nodes stealing can occur.

iii. The WSNs are susceptible to attacks of consumption of resources. Attackers can waste network bandwidth and frequently send packets to exhaust a node battery.

Due to these factors, it's essential for the sensitive digital information to be securely transmitted over the sensor networks.

2. Security Requirements

WSNs are used in lots of applications with different security requirements. E.g., an application for environmental monitoring demands less security whereas; battlefield monitoring applications demands high security levels. For environmental monitoring applications in-network processing is vital to reduce the network contention (Ahmed, 2009).

According to Sharma, Chaba & Singh, 2010 the security requirements or services are such as; availability, authorization, authentication, confidentiality, integrity, non-repudiation, data freshness, robustness, self-organization and time synchronization.

a. Availability

This is a security service that checks to see if a given node can utilize the resources and also if the network is available to communicate messages. The WSN can be endangered if the sink (base station) or cluster head fails. Therefore availability is crucial for a network to be operational (Padmavathi & Shanmugapriya, 2009).

The availability security service for WSNs has been looked at in-depth from the Denial-of-Service (DoS) type attacks dimension in addition, properties for connecting WSNs as concerns availability has also been studied in great length (Uluagac et al., 2008).

b. Authorization/Access control

This ensures that only authorized users and devices have access to the WSN.

c. Authentication

This security requirement ensures that there is valid communication from a given node to another node; this means an untrusted node cannot pretend as a trusted node (Rajkumar.et al., 2012.).

d. Confidentiality

Confidentiality is referred to as the capability to hide messages from any given adversary (attacker) to ensure any message transmitted through the WSN is confidential (Padmavathi & Shanmugapriya, 2009). In case a rival, accesses the content, he should not be able to decode the messages exchanged in the network.

To provide a confidential security service to WSNs applications you require the use of cryptographic mechanisms such as encryption techniques. Generally, two kinds of encryption approaches are used;

i. Symmetric encryption
ii. Asymmetric encryption.

Symmetric encryption uses the identical key at both the sender and receiver nodes to encrypt and decrypt the information from plain text to cipher text and vice versa. While asymmetric key based encryption, uses dissimilar keys, one public and the other private which are used to convert and recover the information (Uluagac et al., 2008).

There is no single encryption mechanism that one can claim is better than another as it is basically a matter to do with size of the key and the computational effort that can be used to break the encryption algorithm.

Another facet to confidentiality research in WSNs is on issue of designing efficient key management schemes. The keys must always be available to all the nodes communicating and this ensures privacy of channels is maintained (Uluagac et al., 2008).

The process of managing keys involves two basic steps;

i. Key generation
ii. Keys distribution

This process is triggered by keying events like network attack. However, it's not a simple task and in a number of applications it may be overwhelming operation to go to each and every sensor considering their numerous numbers and updating of their keys, for-example underwater sensor applications. Therefore, management of keys intelligently is essential for WSNs (Uluagac et al., 2008).

e. Integrity

Integrity is basically confirmation of a message not being changed, tampered with or altered (Padmavathi & Shanmugapriya, 2009). On the message content a content digest is appended to provide integrity of content exchanged. On receipt of message by the receiving node content digest is checked to confirm that content digest computed and received digest are equal. Once confirmed to be equal or same then it's treated as a legitimate message. Hashing algorithms are used to create content digests (Uluagac et al., 2008).

There are several algorithms for hashing available and these algorithms do not usually require the keys presence unless designed specifically to work with keyed-hashing for-example Keyed-Hashing for message Authentication Code (HMAC) and Cipher-based Message Authentication Code (CMAC) (Uluagac et al., 2008).

Integrity service checks data staleness since some decisions for some applications depends on whether the data is recent or it's not. For- example, waters of a given territory can be protected with sinks detonated mines. Message freshness and its accurate timing from the sensor nodes in this kind of application are critical (Uluagac et al., 2008).

Integrity service also is meant to provide a mechanism for recovery from any content that has been altered (Uluagac et al., 2008).

f. Non-repudiation

Non-repudiation security service ensures that a node cannot deny the messages it has sent (Rajkumar et al., 2012). To offer non-repudiation service digital signature scheme (DSS), which utilizes encryption methods, can be used. DSS can use either symmetric or asymmetric encryptions (Uluagac et al., 2008).

When you use symmetric encryption the WSN may be in danger of another sensor masquerading as the sensor's original signature. On the other hand, using asymmetric encryption may be expensive. Basically non-repudiation service facilitates the approval by another entity for message sent or received in WSNs. Therefore, a legitimate node, such as the base station (sink) can offer the service (Uluagac et al., 2008).

g. Data freshness

This guarantees that the data over the WSN is current and not replicated

h. Robustness

This guarantees that in the event of some nodes being compromised, the WSN continues to operate.

i. Self-organization

This ensures that the sensor nodes are independent and can be flexible in the event of adding new nodes or some nodes fail. WSNs are basically ad hoc networks; this characteristic makes it prone to security issues. Therefore, in the circumstance self-organization and self-healing is impossible then the damage could be overwhelming.

j. Time synchronization

WSNs applications rely on time synchronization for purposes such as; power conservation, packets end-to-end delay computation, and group synchronization for tracking applications.

k. Secure localization

This is a requirement for the sensor nodes to be able to securely identify its location (Pathak & Quaz, 2017).

3. Attacks on Wireless Sensor Networks

Wireless sensor networks attacks are categorized by different authors as follows;

a) Active attacks and passive attacks. The active attacks modify data and include Blackhole, Sybil, HELLO Flood attack, denial of service and wormhole attack. The passive attacks are such as; attacks against privacy, eavesdropping and traffic analysis (Padmavathi & Shanmugapriya, 2009).

b) According to Sunitha & Chandrakanth (2012), wireless sensor networks attacks are in three categories;

   i. Secrecy and authentication attacks –These attacks are such as spoofing, eavesdropping, and packet replay attacks.

   ii. Attacks on network availability-These attacks are also known as denial-of-service (DoS) attacks.

   iii. Stealthy attack against service integrity-The attacker makes the WSN acknowledge a false data value. E.g. through injection of false data value.

c) Attacks against security mechanism and attacks against routing mechanisms (Pathan, Lee & Hong, 2006)

The major WSN attacks are

i. Wormhole attack

The attacker near a base station tunnels the traffic to a low latency link thus disrupting the traffic

ii. Hello flood attack

This attack happens when assumption is made that the node broadcasting HELLO packets is a genuine neighbor. This can cause a large number of nodes to attempt to use this route, thus sending packets into oblivion.

iii. Blackhole attack

This attack is when all packets are dropped, meaning none is transmitted.

iv. Sinkhole attack

This kind of attack occurs when a malicious node attracts maximum traffic through it

v. Denial of service attack (DoS)

The attacker ensures that the legitimate users don’t gain access

vi. Sybil attack

This is when a node masquerades with multiple identities in the network.

vii. Attacks on information in transit

viii. Selective forwarding

This attack makes some packets to be dropped and others are transmitted

ix. Spoofing

4. Security Challenges in WSN

The universal approach for defense against cyber-attacks is cryptography, but there exists challenges in keeping required level of security and safety of critical data transmitted over wireless sensor network. WSN has myriad of inherent challenges when compared to the conventional computer networks. The table below compares the WSN and the traditional networks.

Table 1: Comparison of WSN and Traditional networks

Wireless Sensor Networks (WSNs)	**Conventional(Traditional) Networks**
Bandwidth is less	More bandwidth
Devices have very little computational power	Comparatively devices have more computational power
Energy is less with wireless	Energy for devices is comparatively high

sensor devices	
Information is mostly transmitted in hop-by-hop	Information is mostly transmitted using end to end
Vulnerable to resource consumption	Not vulnerable to resource consumption
Quite difficult to protect	Comparatively much easier to protect

5. Wireless Sensor Networks Security Protocols

Security protocol is defined as a set of rules that determine how the interaction between peer processes to make available a given security service (Aseri & Singla, 2011). A number of security protocols have been proposed to date, and the most popular for WSN are discussed in this section.

a) SPINS

SPINS was proposed by Perrig et al., 2002, and it's a collection of security protocols optimized for sensor networks. SPINS has two secure building blocks specifically Secure Network Encryption Protocol (SNEP) and ^{u}TESLA. SNEP provides data authentication for two parties, confidentiality of data, and freshness of data while ^{u}TESLA authenticates broadcasts.
Limited storage hurdle is achieved by protocols through the reuse of code for all crypto primitives such as, message authentication code, encryption, and hash random number generator. In addition, to reducing the communication overhead, it shares the common state between communication parties. Semantic security is achieved through SNEP by incorporating counter in both sender and receiver ends. It's important to note that the counter is not incorporated with the message so as to reduce the data transmission rate (Ahmed, 2009). SNEP supports simply base-to-node communication and vice-versa while ^{u}TESLA provides authenticated broadcast. Traditionally to authenticate broadcasts you require asymmetric keys to authenticate the initial packets, but ^{u}TESLA uses symmetric key to provide security with symmetric keys disclosure delayed. Unfortunately with a network of many nodes synchronization is a challenge (Ahmed, 2009).

b) TINYSEC

TinySec is a link layer security protocols for Wireless sensor networks (WSNs), and its main difference with the SPINS is that it doesn't make use of counters. The provision of passive communication (in-network processing) is done by Link layer security among local nodes to eliminate communications that are overlapping with the sink (base station) (Ahmed, 2009).
Karlof et al., 2004 designed TinySec to replace the incomplete Sensor Network Encryption Protocol (SNEP), called TinySec. TinySec is link layer security architecture for WSNs and it offers security services such as access control, confidentiality, and message integrity.

Integrity and access control are ensured through authentication method referred to as MAC (Message Authentication Code), and confidentiality through encryption method referred to as CBC (Cipher Block Chaining) mode. A unique initialization vector (IV) provides semantic security for each invocation of the encryption algorithm. This means there should be no guessing of any no or yes question as regards a given message by adversaries for no more than 50% probability. Initialization vectors (IVs) provides variation to encryption and this is necessary when variation of messages to be encrypted are few (Karlof et al., 2004).

c) MiniSec

It consumes low energy as compared to TinySec and it's used at the network layer.

MiniSec uses offset Codebook Mode (OCB) as its block cipher mode of operation.

d) Link-layer security protocol (LLSP)

Lighfoot et al., 2009; designed a Link-Layer Protocol (LLSP) and the goal was to develop a protocol with low energy requirements as compared to TinySec. LLSP ensures message confidentiality, message authentication, replay protection and access control. LLSP supports early rejection capability in addition, it has low performance overhead. However maintaining a large network is difficult with in node counter due to that it has low scalability.

e) Light weight security protocol (LISP)

LiSP is a lightweight security mechanism that supports key renewability and puts into balance the need for security and consumption of resources. LiSP from time to time renews the shared key to solve the problem of reuse of key stream-reuse and maximize energy efficiency and scalability. LiSP also supports distribution of keys which is reliable (Park & Shin, 2004).

LiSP is efficient in terms of energy and is robust to denial of service (DoS) attacks, since it doesn't require retransmitting or any control packets. LiSP has a joint authentication and recovery algorithm for rekeying, where Key -Server (KS) from time to time a new key is broadcast before it's used for encryption and decryption. The key received is authenticated by client node and then recovers all keys that have been missing (Park & Shin, 2004).

The goal of LiSP is to offer a lightweight security solution for a large-scale network of resource-limited sensor devices. LiSP divides the whole network into clusters and selects a Group-head (GH) for each of them to offer scalability for a large number of sensors (Park & Shin, 2004).

f) Location aware end-to –end security (LEDS)

LEDS offers location aware end-to-end security. Several sensing nodes endorse genuine event reports in LEDS and are encrypted with a unique secret key which is shared between the sink and event sensing nodes. LEDS provides end-to-end authentication and en-route filtering capability to deal with the recognized attacks for injection of data. If there are no more than a given stated number of compromised nodes in each single area of interest, LEDS assures that a fake or false data report from a given cell can be filtered by genuine in-between sink or the nodes (Ren, Lou, & Zhang, 2008). LEDS provides location aware key management. LEDS can be used in both small and large networks and the key numbers increases with size of the cell. In addition, LEDS doesn't support dynamic topology. LEDS puts the network into several cell regions and when an event occurs in a given region, the event should be sensed by several nodes (Ahmed, 2009).

Data availability is assured by LEDS because it deals with both report disrupting attack and selective forwarding attack at the same time. Wireless links are broadcast in nature and so LEDS adopts one node to many nodes data forwarding approach, this ensures LEDS reports are authenticated by several next-hop nodes separately. This means that no reports disappear due to being dropped by a single node. (Devi et al., 2011)

LEDS ensures a very high level of security without considering the costs for communication and computing in addition LEDS provides data confidentiality and node capture attacks to a reasonable level (Ahmed, 2009).

g) Localized encryption and authentication protocol (LEAP)

Zhu et al., 2003 proposed LEAP as a key management protocol for WSNs, after observing that different kinds of messages transmitted in wireless sensor networks (WSNs) demands different security

requirements. The key design aims of this protocol are; robustness, lightweight, survivability and energy efficient operation.
LEAP has four (4) different keying mechanisms which are;

i. Individual keys-This key are shared between every node and sink (base station). This provides confidentiality in communication between individual nodes and base station.
ii. Group key- Encrypted messages from the base station are sent using this key to the whole wireless sensor network. They are used to send queries to the network nodes.
iii. Cluster key-It's like group key but it's shared between a node and its neighbor. It's used to broadcast messages locally in a secure manner.
iv. A pair wise shared key- This key is shared by all nodes with their closest (immediate) neighbors.

h) ZIGBEE

It uses three network devices; Zigbee coordinator which initiates communication, stores information and bridges various networks. Zigbee router links various devices and provides multi-hop communication. Finally the Zigbee end devices which collect data and communicates with other components (Bhalla, Pandey & Kumar, 2015). Zigbee has two modes of operation, residential mode for applications with low security demands and commercial mode for applications with high security demands (Boyle & Newe, 2007).

i) Modified SPINS

It works in three phases namely; data broadcasting phase where source node first broadcasts ADV message to its neighbor to send new data to a specific node, data requesting phase where after receiving ADV message each node has to verify if it has enough energy to perform tasks and finally data transmission phase where the source node sets up the route to send data (Dutta, Gupta & Paul, 2014).

j) Intrusion tolerant routing protocol for wireless sensor networks (INSENS)

This protocol leverages on SPINS protocol concept. It utilizes keyed message authentication codes (MAC) for integrity purposes. It uses a one-way hash chain which provides one-way sequence numbers for loose authentication of the base station.

Table 2: Summary of Protocols

Security protocol	**Security services provided**	**Security attacks protected**	**Strengths**	**Limitations**
SPINS	• Data confidentiality • Authentication • Data freshness • Integrity	• Eavesdropping • Spoofing • Message replay attack	• It has low communication overhead • Offers Semantic security.	• Use of counters • Blind forward • Data inaccessibl e • Cannot guard against DoS attacks
TINYSEC	• Data confidentiality • Authentication • Data freshness • integrity	• Spoofing • Message replay attack	• Energy efficient as compared to SPINS • Low memory usage	• Cannot guard against resource consumpti on attacks, node capture and replay attacks
MiniSec	• Freshness • Authentication • Data Confidentiality	• Spoofing • Message replay attack	• Low energy consumption as compared to TinySec and SPINS • Provides high security at low power consumption	• Don't provide data integrity • Cant assure data availability • Defenseles s against DoS attacks
LEAP	• Authentication • Confidentiality	• HELLO flood attack • Sybil attack • Wormhole attack • Reduces selective	• Supports various communication patterns • Supports in-	• Assumptio n that sink node is never

		forwarding attack effect • Sinkhole attack •	networking processing • Robust against attacks • Energy efficiency • No message fragmentation •	compromised
Zigbee	• Freshness • Authentication • integrity	• Sybil attack • Sinkhole attack • Wormhole attack	• It's scalable • Consumes little energy	• Prone to attack from unauthorized nodes • Provides high security at high power consumption
LEDS	• Data Authentication • Data availability • Data confidentiality	• Prevents node capture attacks • DoS Attacks • Selective forwarding attacks	• Offers location aware end-to-end security • Can be used in small and large networks • Highly robust against DoS attacks	•
LLSP	• Provides message authentication • Provides access control • Provides message confidentiality • Provides message confidentiality	• Protection against replay attacks	• Lesser time to transmit packets as compared to TinySec. • Lesser energy consumption as compared to TinySec • It's secure and computationally efficient • Provides message semantic security at minimal cost	• Can't assure data availability • It has low scalability

LISP	• Authentication • Data Integrity • Access control • Confidentiality • Availability	• DoS Attacks • Protection against malicious nodes • Protection against replay attacks	• Energy consumption efficient • Robust to DoS attacks • Can be used for large scale WSNs	• Security intermediate, requires an Intrusion Detection System (IDS) for better security.
Intrusion tolerant routing protocol for wireless sensor networks (INSENS)	• Message authentication • Integrity	• Resilient to DoS attacks	• Limits flooding of messages • Scales to large networks • Enables secure joining and leaving • Allows multipath routing to multiple base stations.	• Damage can be very big if the attack is around the base station.
Modified SPIN	• Data confidentiality • Authentication • Data freshness • integrity	• Eavesdropping • Spoofing • Message replay attack	• No blind forwards • Data is accessible • Energy efficient as compared to SPINS	• Some nodes are used more than others therefore they are destroyed earlier than others.

6. Conclusion

In the face of myriad of challenges facing WSNs, designers of WSNs are faced with hard choice of security protocol to implement. This paper has summarized the different security requirements for WSNs, the security protocols and the security requirements they achieve and of importance a summary has been given to show the strengths and limitations of each of the security protocol. This will go in handy to help ease the process of choice of security protocol to be implemented in various applications.

REFERENCES

Ahmed, A. S. (2009, April). An evaluation of security protocols on wireless sensor network. In *TKK T-110.5190 Seminar on Internetworking*.

Aseri, T. C., & Singla, N. (2011). Enhanced Security Protocol in Wireless Sensor Networks. *International Journal of Computers Communications & Control*, *6*(2), 214-221.

Bhalla, M., Pandey, N., & Kumar, B. (2015, October). Security protocols for wireless sensor networks. In *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on* (pp. 1005-1009). IEEE.

Boyle, D., & Newe, T. (2007, March). Security protocols for use with wireless sensor networks: A survey of security architectures. In *Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on* (pp. 54-54). IEEE.

Devi, S. A., Babu, R. V., & Rao, B. S. (2011). A new approach for evolution of end to end security in wireless sensor network. *International Journal on Computer Science and Engineering*, *3*(6), 2531-2543.

Dutta, R., Gupta, S., & Paul, D. (2014, December). Energy efficient modified spin protocol with high security in wireless sensor networks using tossim. In *Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on* (pp. 290-294). IEEE.

Karlof, C., Sastry, N., & Wagner, D. (2004, November). TinySec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems* (pp. 162-175). ACM.

Lighfoot, L.E., Jian R. & Tongtong L.(2009). An Energy Efficient Link-Layer Security Protocol for Wireless Sensor Networks. *IEEE EIT Proceedings* (pp 233-238).

Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv: 0909.0576.*

Park, T., & Shin, K. G. (2004). LiSP: A lightweight security protocol for wireless sensor networks. *ACM Transactions on Embedded Computing Systems (TECS)*, *3*(3), 634-660.

Pathak, P. & Quaz, M,A. (2017), Issues, Challenges and Solution for Security in Wireless Sensor Networks: A Review International Journal of Electrical, Electronics ISSN No. (Online): 2277-2626 and Computer Engineering 6(1).

Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference* (Vol. 2, pp. 6-pp). IEEE.

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless networks*, *8*(5), 521-534.

Ren, K., Lou, W., & Zhang, Y. (2008). LEDS: Providing location-aware end-to-end data security in wireless sensor networks. *IEEE Transactions on Mobile Computing*, *7*(5), 585-598.

Sharma, R., Chaba, Y., & Singh, Y. (2010). Analysis of security protocols in wireless sensor network. *International journal of advanced networking and applications*, *2*(3), 707-713.

Sunitha, K., & Chandrakanth, H. (2012). A survey on security attacks in wireless sensor network. *International Journal of Engineering Research and Applications (IJERA)*, *2*(4), 1684-1691.

Uluagac, A. S., Lee, C. P., Beyah, R. A., & Copeland, J. A. (2008, October). Designing Secure Protocols for Wireless Sensor Networks. In *WASA* (pp. 503-514).

Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *2*(4), 500-528.

J.G Ndia received a MSc. Data Communications from KCA-University, Kenya in 2013. He is currently pursuing a PhD in Information Technology at Masinde Muliro University of Science and Technology, Kenya and serves as a Tutorial Fellow at Murang'a University of Technology. His current research interests are in the area of Network Security and Software Engineering.