SURVEY ON WIRELESS SENSOR NETWORK SECURITY

By
Shriya Rajan

Amity University, Greater Noida Campus

***Abstract*:** Wireless Sensor Network (WSN) is a progressive technology that shows great promise for various futuristic applications. It is already in use in critical monitoring and control applications around the world. However, security is crucial to the success of applying WSN. While the deployment of sensor nodes in unattended environment and the inherently unsecure nature of wireless medium challenge the integrity of transmitted data, the power and processing constraints of sensor nodes make conventional security solution impractical. This paper tends to outline various aspects of wireless sensor network security. The introductory section gives brief overview of WSN and outlines the basic security goals. It then discusses various attacks in WSN and highlights the importance of symmetric cryptographic primitives for providing security in WSN.

***Keywords*:** Wireless Sensor Network (WSN), data models, security goals, attacks, symmetric cryptographic primitives, block ciphers and stream ciphers.

INTRODUCTION

Wireless Sensor Networks are used to exchange information between an application platform and sensor nodes. This exchange takes place in a wireless fashion [2]. The main purpose of WSN is to serve as an interfaceto the real world, providing physical information [4] for further analysis and computation. Possible applications of WSN include environment/earth sensing area monitoring, health care monitoring, traffic surveillance and industrial monitoring and smart home application. The devices in WSN are independent, not controlled by human users [4]. They are often deployed in large quantities and in hostile environments. Also, the devices are much more constrained in terms of battery life and processing power so it can only perform certain simple, predefined sets of tasks [4].

A. *Components*

The major components of WSN are the sensor nodes and the base stations. The sensor nodes interact with the physical system and get the information using its built-in sensors, process the information using computational capabilities and communicate with other nodes in its surrounding. All sensor nodes are battery-powered and can operate independently. They can also collaborate with other nodes in pursuing a common goal. The base station consists of the application platform and is a centralized component that is used for accessing the services provided by the sensor network. [4] All information received by the wireless nodes is aggregated by the gateway and forwarded to the application [2]. The data coming from the sensor nodes, as well as the commands issued to those nodes, go across the base station. [4]

B. *Data Models*

The data models of WSN characterize and describethe interaction between the sensor and the application.The data models or the services provided by WSN can be classified into three major categories [2]:

Period Sampling (monitoring), event driven (alerting) and store and forward. For the first case, sensor nodes constantly monitor certain features of their surroundings (ex. temperature) and the sensor data acquired from a number of sensor nodesis forwarded to the base station on a periodic basis. In the second case, sensors check whether a specific event or condition(ex. fire alarms) has occurred, alerting the users of the system when an alarm

is triggered. In the last case, data can be stored or even processed by a sensor node before it is transmitted to the base station. The network can be asked about levels of a certain feature, providing information "on demand" instead of immediately transmitting every sample as it is acquired. [2, 4]

The more researchers try to develop further cost and energy efficient computing devices and algorithms for WSN, the more challenging it becomes to fit the security of WSN into the constrained environment. Established approaches from other network types are often hard to implement due to the special characteristics of WSNs [3].

The following section outlines the basic goals of security in WSN.

SECURITY GOALS

The idealistic security requirements in any WSN include data integrity, authenticity, confidentiality and continuous availability.

A. *Data Confidentiality*

It means that the data transferred in the network cannot be read by anyone but the intended defined set of recipient. [6] Encryption of data with a key that is shared amongst all authorized people is typically used to achieve confidentiality in open networks. [3]

B. *Data Integrity*

It is needed to ensure that any message received is known to be exactly the message that was sent, without modifications of the content. [6] It addresses the threat of unauthorized manipulation of data. Usually keyed hash algorithms are used to generate a fingerprint of the message that can be verified only when the corresponding secret key in known. [3]

C. *Data Authentication*

It ensures that a message that claims to be from a given source is,infact, from that source.[6] It is the proof of a claimed identity during communication. In the context of WSNs, challenge response protocols are one of the most meaningful methods to provide authorization. [3]

D. *Data Availability*

It determines whether the network is available for the message transfer and whether a node has the ability to use the resources. Thus, availability of data is essential to allow correct provisioning of services. [5]

The above section discusses the primary security goals in WSN. However, achieving these goals is not any easy task for WSN [4] as it is inherently vulnerable against various security attacks. The next section outlines the various attacks that can occur on WSN.

ATTACKS ON WIRELESS SENSOR NETWORK

The sensor nodes in WSN are highly constrained in terms of memory, computational capabilities, communication bandwidth and battery power. Additionally, it is easy to physically access such nodes because they are located near the physical source of the events, and they usually are not tamper-resistant due to cost constraints. Also, the wireless link is highly susceptible to external and internal attacks. As a result, WSN has to face various threats that may hinder its functionality and nullify the benefits of using its services. [4]

These threats are:

1) ***Eavesdropping*:** It is an attack against privacy. [5] It is when an adversary retrieves data from the transmitted packets that are sent. The data collected can be later analyzed to extract sensitive information. [9]

2) ***Denial of Service attack*:** It refers to an adversary's attempt to disrupt, subvert, or destroy a network. [5] A DoS attack can be any event that diminishes or eliminates a network's capacity to performits expected function. [1]DoS attack on WSN may take several forms like jamming and exhaustion of power. [4]

3) ***Jamming attack*:** Attack in which an adversary jams the communication channel and avoids any member of the network in the affected area to send or receive any packet. [4] The attacker has the potential to disrupt the entire network provided the jamming sources are randomly distributed in the network. [1]

4) ***Exhaustion of power*:**In this an attacker repeatedly requests packets from sensors to deplete their battery life. [4]Unless the retransmissions are discovered or prevented, the energy reserves of the transmitting node and the surrounding will be quickly depleted. [1]

5) ***Sybil attack*:** It is a case where one node presents more than one identity to the network.[1]A node that wishes to conduct the Sybil attack can adopt a new identity by creating a new identity or by stealing the identity of existing node. [4]

6) ***Node replication attack*:** In this an attacker seeks to add a node to an existing sensor network by copying the node identity of an authorized node. [5] It is duplication of sensor nodes. [4]

7) ***Spoofed routing information*:** It is an attack against a routing protocol in any network to target the routing information. An attacker may spoof, alter or replay routing information. The disruption due to this include the creation of routing loops , attracting or repelling network traffic from selected nodes, extending and shortening source routes, generating fake errors messages,partitioning the network and increasing end- to- end latency. [1]

8) ***Selective forwarding*:**it includes selective forwarding of the packets that traverse a malicious node depending on some criteria. [4] Specific form of this attack is the black hole attack in which a node drops all messages it receives. [1]

9) ***Wormhole attack*:** In this an attacker captures packets at one location and replays them in another location. [4]

10) ***Sinkhole attack*:** In this attack the adversary attracts the surrounding nodes to choose the compromised node, which is accessible to the adversary, as the next node to route their data through. [1]

11) ***Hello flood attacks*:** It is the creation of false control packets during the deployment of the network. [4] The attackers with the high radio transmission range and processing power sends HELLO packets to a number of sensor nodes. The sensors are thus influenced that the adversary is their neighbour. As a result, while sending the information to the base station all of these nodes attempt transmission to the attacking node. [1]

12) ***Acknowledgment spoofing*:** Routing algorithms used in the sensor networks sometimes require acknowledgments to be used. [1] In this case an attacking node creates false acknowledgement information and sends it to the neighbouring nodes. [4]

TABLE I
Attacks and Counter Measure in Wireless Sensor Networks.

Attacks	Countermeasures
Eavesdropping Jamming Node Tampering	Sleeping/hiding, Spread spectrum communications, Encryption, Tamper proofing
Collision Exhaustion	Intrusion Detection, Error-correcting code, Rate limitation
Spoofed routing information Selective Forwarding Sybil Node replication Wormhole Sinkhole Hello Flood Attacks Acknowledgment Spoofing	Secure routing protocols, Authentication, Verify the bidirectional link, False routing information detection, Using Synchronized Clocks, Probing, monitoring,

SECURITY PRIMITIVES

Application of cryptographic protocols is an approach to protect a network against threats like eavesdropping, unauthenticated access to the network or change of transmitted messages [3]. Selecting the most appropriate cryptographic method is vital in wireless sensor networks as the cryptographic method used should meet the constraints of sensor nodes.

The cryptographic primitives are fundamentally divided into following categories:

A. *Symmetric Primitives*

The symmetric primitives or symmetric key ciphers consist of an encryption and a decryption transformation using the same key as input. The two types of symmetric key ciphers are block ciphers and steam ciphers. While block ciphers operate on fixed length input blocks, the input of stream ciphers is bit oriented. Message Authentication Codes (MACs) that are basically arbitrary length hash function with additional key input are also considered as symmetric primitives. The major advantage of symmetric key primitives is their limited computational complexity. The algorithms can be performed in reasonable time on small microcontrollers or small dedicated hardware modules can be designed to increase performance or decrease energy consumption. Since security of encryption schemes using symmetric key encryption is established as long as the key is a shared secret between the communication partners, such schemes are often referred to as secret-key cryptosystems. [3]

B. *Asymmetric Primitives*

The asymmetric primitives are a combination of encryption function and a decryption function that use different key inputs. The two key values are typically generated together, and often one of the two keys is published (public key) while the other is kept secret (private key). It is computationally infeasible to deduce the private key from the public key. Asymmetric primitives allow secure communication although one of the two key values was published. Therefore, they are often referred to as public-key cryptosystems. The major disadvantage of asymmetric cryptography is the high computational effort that is necessary to compute the algorithms. Furthermore, the energy consumption due to the higher computation effort is often not negligible. The increased key length also results in higher communication effort to perform cryptographic protocols with asymmetric primitives. [3]

The security of asymmetric cryptography depends on the difficulty of a mathematical problem and the resulting algorithm consumes considerably more energy than symmetric key ciphers, which are constructed by iteratively applying simple cryptographic operations. Hence in wireless sensor networks, the symmetric key cipher is typically utilized to encrypt data during the transmission of sensor data, conforming to the limited energy source in the sensor device [8].

SYMMETRIC CRYPTOGRAPHIC PRIMITIVES

The following section gives a brief description of the two types of symmetric key ciphers, block ciphers and stream ciphers.

A. *Block Ciphers*

Block Ciphers are symmetric-key primitives which operate on blocks with a fixed number of bits. A transformation is specified which modifies the input data block using the secret key and outputs the ciphertext. Decryption is the inverse operation which allows to

recover the plaintext from the ciphertext and the secret key. [3]

Popular block ciphers are:

1) ***Data Encryption Standard (DES):*** this algorithm was standardized in the year 1976 by National Institute of Standards and Technology (NIST). It has been the most important block cipher for several decades. [3] DES has a block size of 64 bits and a key size of 56 bits. An extension to DES, Triple DES triple-encrypts each block.

2) ***Advanced Encryption Standard (AES)*:** the Rijndael algorithm was selected as the winner of an open selection process by NIST and has been standardized in the year 2001. Due to its flexibility, the AES algorithm can be implemented in software as well as in hardware very efficiently. It has a fixed block size of 128 bits and a key size of 128,192,256 bits. The AES algorithm security has been scrutinized by a large number of cryptanalytic experts. Besides its good security properties it has the advantage that it can be implemented on all classes of devices very efficiently.[3]

3) ***Serpent*:** In comparison to Rijindael, which has the advantage of its efficient implementation to various platforms, Serpent has a higher security margin and is therefore much slower.[3]

4) ***IDEA*** (*International Data EncryptionAlgorithm*): encrypts 64-bit ciphertext blocks, using a 128-bit input key. It is a sufficiently strong block cipher and is used in Pretty Good Privacy (PGP) protocol. [3]

B. *Stream Ciphers*

A stream cipher encrypts plaintext one byte at a time. In this a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random. A pseudorandom stream is one that is unpredictable without knowledge of the input key. The output of the generator, called a keystream, is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR operation. With a properly designed pseudorandom number generator, a stream cipher can be as secure as block cipher of comparable key length. The primary advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers. [7]

The most famous stream cipher is RC4.It is a variable key-size stream cipher with byte-oriented operations. RC4 is widely applied in security protocols like SSL/TLS (Secure Sockets Layer/Transport Layer Security) and WEP (Wired Equivalent Privacy) but has been shown to have some weakness. [3, 7]

Using stream ciphers in WSNs could be an alternate to block ciphers. Especially on sensor nodes where little data is sent at a certain time the ability to encrypt only a few bits could lead to a significant performance gain. [3]

CONCLUSION

In this paper, we have surveyed the security issues in wireless sensor network starting with the constraints in WSN, followed by the attacks and finally an overview of symmetric cryptographic primitives has been given. The most commonly used representatives of block ciphers and stream ciphers are described.

Wireless sensor network is critical to extending the reach of internet infrastructure to everything. Its applications are only limited by ones imagination and therefore to support this diversity of applications, the development of network techniques comprising of efficient and secure communication protocols, algorithms, designs and services are needed.

REFERENCES

[1]. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of SecurityIssues in Wireless Sensor Networks," *IEEE Commun. SurveysTutorials*, vol. 8, pp. 2–7, year 2006.

[2].J.Cecilio and P.Furtado, "Wireless Sensors in Heterogeneous Networked Systems Configuration and Operation Middleware",XVIII, pp.6,15, Springer, 2014

[3].M.Aigner, M.Feldhofer, S.Tillich, "Symmetric Primitives" in Wireless Sensor Network Security, IOS press,2008.

[4]. J.Lopez and J.Zheu, "Overview of wireless sensor network security" in Wireless Sensor Network Security, IOS press, 2008.

[5]. G.Padmavati and D.Shanmugapriya, "A Surveyof attacks security mechanism and challenges in Wireless Sensor Networks" *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 4, No. 1&2,2009.

[6]. Kris Pister& Johnathon Simon, article on "Secure Wireless Sensor Networks Against Attacks" in Electronic Design, April 14, 2014.

[7]. W. Stallings, *Cryptography and Network Security Principles and Practices*,Fourth Edition, Pearson Education, Prentice Hall, 2010.

[8]. X.Zhang, H.Hayes and C.Li, "Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks",2010

[9]. Kai Xing, ShyaamSundharRajamadam Srinivasan, Manny Rivera, Jiang Li, Xiuzhen Cheng, "Attacks and Countermeasures in Sensor Networks: ASurvey", *Network Security*, Scott Huang, David MacCallum, and Ding Zhu Du(Eds.) pp. 4-21 ©2005,Springer