International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V68I1P106

Volume 68 Issue 1, 26-30, January 2020

Original Article

Security in Wireless Sensor Networks

S.Sabeena[1], R.Iniya[2]

[1]*Assistant Professor, Department of Commerce, Nehru Arts and Science College,* Coimbatore, India
[2]*Student, Department of Commerce, Nehru Arts and Science College, Coimbatore, India*

Received Date: 10 November 2019
Revised Date: 04 January 2020
Accepted Date: 07 January 2020

Abstract *- The idea of Wireless Sensor Networks (WSN) was brought about by very small sensor nodes that are capable of sensing, data processing and wireless communication. Without the aid of any pre-existing network infrastructure, WSN provides network connectivity. In a complex environment, WSN ensures large scale real-time data processing. As WSN technologies are facing tremendous growth in recent years, security has become a critical issue. In this paper, we presented the security issues involved in the WSN systems and also paved the way for the corrective measures of such issues.*

Keywords *- Wireless Sensor Networks, security restrictions, WSN attacks, security solutions.*

.

I. INTRODUCTION

The wireless sensor network technology is emerging as an essential part of modern communication methods as it offers low-cost solutions to a variety of real-world challenges [1]. The main advantage of WSN is that it connects small devices which are capable of sensing and communication. The WSNs are considered as an innovative technology that changes the way of interaction with the physical world like mobile communication changed the way we communicate with each other in the olden days.

Because of the inherent limitations in communication and computing, sensor networks face unique security challenges. The sensor networks are a victim of various attacks due to their deployment nature. The deployment nature arises when they have physical interaction with the surroundings, people and other objects resulting in various security threats. The sensor networks may be deployed on the battlefield, habitat monitoring and farming, measuring traffic flow, security of key landmarks, buildings and bridges [2]. The major WSN attacks include internal versus external attacks, active versus passive attacks and layer-based attacks [3]. The sensor networks are being protected by various defence mechanisms like cryptography, key management protocols, intrusion detection systems, secure data aggregation, secure routing, and secure localization and trust management system. The below diagram gives the pictorial description of wireless sensor networks;

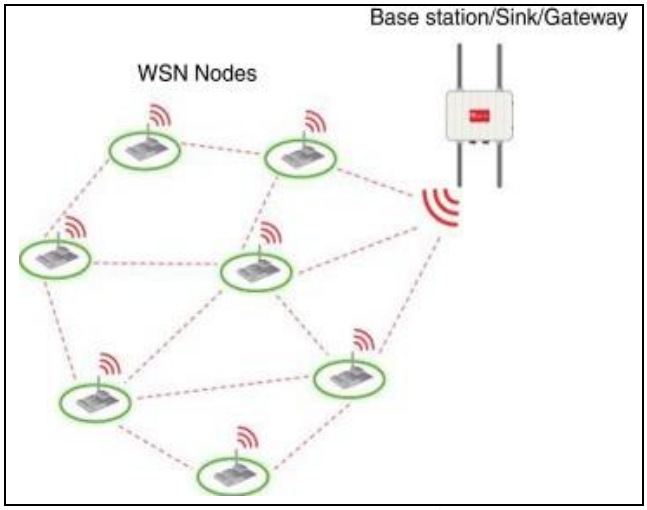

Fig. 1 Pictorial description of WSN

This paper gives a detailed study of the attacks and threats arising to WSN systems and possible countermeasures for such attacks. This article is organized as follows; the first section gives a brief introduction to WSN technologies and their nature of functioning mechanisms. The second section lists the limitations and restrictions in WSN systems. Third section spots out the various kinds of attacks happening in WSN technology. The fourth section lights up the security solutions for various WSN attacks. The final section concludes the paper by giving an overview of various WSN attacks and countermeasures for such attacks.

II. SECURITY RESTRICTIONS

The restrictions in WSN security are comparatively higher than the traditional networking systems. It is important to know clearly about the constraints in WSN security to overcome such limitations. The restrictions in WSN security may cause damage to the sensor nodes, which is the vital functioning device in WSN systems. The transmission of information may be interrupted in the middle stage when a security issue arises. The following are some of the restrictions in WSN security;

A. Memory and power restrictions

A sensor is a very small device, so it cannot offer huge space memory and storage. Therefore it is necessary to build the tiniest code for the security algorithms in order to provide an effective security mechanism. Energy may be considered as the ultimate restriction for the wireless sensor capabilities [4]. If any of the sensor nodes are deployed in the sensor networks, it costs a huge operating cost to replace the deployed sensor nodes. Storage and power source plays a major role in WSN functioning.

B. Unreliable communication

The security of the sensor networks depends upon the defined protocol, and such protocol relies on communication systems [15, 16]. The following are the main parameters for unreliable communication.

a) Latency: Latency is the time taken to transfer information in sensor networks. Sometimes the transmission of data may be delayed due to various reasons

b) Conflicts: There may be a clash of data in between the transmission process.

c) Unreliable transfer: The unreliable delivery is the one that will not notify the user if the transmission process fails.

C. Security requirements

The security requirements for wireless sensor networks include the following;

a) ***Confidentiality:*** The encryption method is used to maintain the confidentiality of data. The radio spectrum used in the sensor network is an open resource and can be accessed by anyone who is equipped with a proper radio transceiver. It is a major problem in keeping the confidentiality of data.

b) ***Authentication:*** The receiving node of the transmitted data should ensure that the data is sent from a reliable source [4]. Authentication gives the assurance of the identities of communication that took place.

c) ***Integrity:*** Data integrity gives
Assurance that the transmitted data is not changed either due to malicious code or by accident. The standard approach for ensuring data integrity is the use of a message integrity code.

d) ***Self-Organization:*** The sensor nodes in WSN are capable of self-organizing and self-healing. Due to this ability of sensor nodes, there is no fixed infrastructure available for WSN network management.

e) ***Data freshness:*** Sometimes, the potential adversary can execute a replay attack using the old key in the place of a new key. In such cases, data freshness ensures that the data is recent and no old data key is used.

III. WSN ATTACKS

It is hard to protect the sensor nodes of WSN as they are located in a risky and hostile environment. WSNs are easier victims of many security attacks and threats [5]. In case of the absence of the above-mentioned security requirements, the WSNs may face a lot of security issues. The attacks may occur in various situations. The following are some of the major circumstances in which the WSN attacks occur;

A. According to the capability of the attacker

a) ***External vs Internal attacks:*** External attacks arise due to the nodes which are not authorized to WSN. The outsider will not have legal access to the cryptographic materials of the sensor networks. The external attacks in WSN may lead to snooping of data transmissions in WSN [4]. On the other hand, internal attacks happen when the genuine nodes of WSN function in an unintended way. The internal attacker may be a lawful member in the sensor network who seeks to interrupt the operations and manipulate the organizational assets.

b) ***Passive vs Active attacks:*** Passive attacks may be meant for the eavesdropping of packets exchanged in the WSN, whereas active attacks include the creation of a false stream, which also involves some modifications of the data stream.

c) ***Mote class vs Laptop class attacks:*** Mote class is the kind of attack in WSN by the opponent using certain nodes of similar capabilities like the network nodes. In laptop class attacks, the opponent will use more powerful devices like laptops and cause harmful effects to the sensor networks compared with the malicious sensor code.

B. Attacks on a computer system or network can be categorized into the following;

a) ***Interruption:*** The purpose of interruption is to execute Denial of Service (DoS). The interruption may include physical capturing of nodes, message corruption and insertion of malicious code. Interruption may be defined as an attack on the availability of the network.

b) ***Modification:*** Attacks on the integrity of data is termed modification [14]. Any unauthorized parties not only access the data but also cause changes in it [4]. The main objective of modification is to confuse the parties within the communication protocol.

c) ***Interception:*** Interception is the attack on the confidentiality of data. The opponent compromises the sensor networks to gain unauthorized access to

sensor nodes or data stored within the sensor networks.

d) ***Fabrication:*** Fabrication is the attack on authentication. It causes a threat to the message authenticity. The opponent tries to unlawful implant data and reduce the reliability of the information contained in the sensor network.

e) ***Host-based attacks:*** It is further categorized into software compromise, hardware compromise and user compromise. Breaking the software running on the sensor nodes is involved with the software compromise [6]. Hardware compromise includes tampering with the hardware to extract the program code, data and keys stored in the sensor nodes. Compromising the users of WSN by cheating the users to reveal the user information like passwords and keys to their sensor networks.

f) ***Network-based attacks:*** It consists of layer-specific compromises and protocol-specific compromises. These kinds of attacks include an attack on the information during transmission. The attacker takes an unfair advantage in the usage of networks.

C. Layer based attacks

There may be various attacks in WSN layers even though the communication protocol for WSN has no standard layered architecture. These attacks may arise in various WSN layers like physical layer, network layer, data link layer, application layer and transport layer [9]. Each layer is a victim of different kinds of attacks. Such issues can be thrown out by different defence mechanisms in WSN technology. The following are some of the layers facing different attacks;

a) ***Physical layer:*** attacks in the physical layer are tampering, jamming and radio interference.

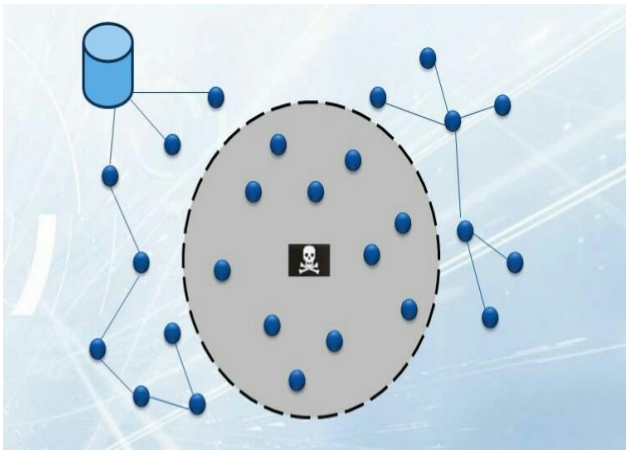

Fig. 2 Attacks in a physical layer

b) ***Datalink layer****:* Attacks in this layer are collision, Sybil attacks, exhaustion, unfairness, interrogation.

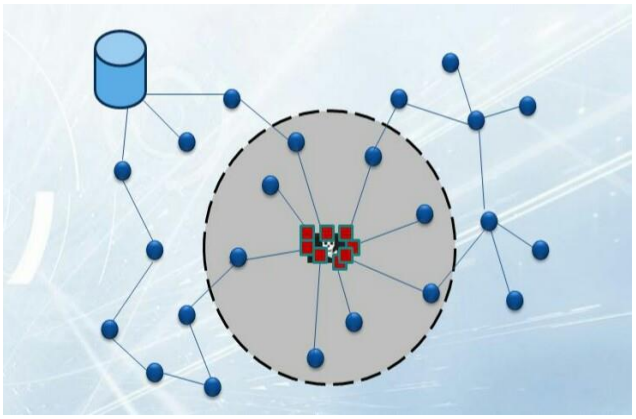

Fig. 3 Attacks in data link layer

c) ***Network layer:*** Attacks include HELLO flood, warm hole, node capture, sinkhole, selective forwarding, misdirection, internet smurf, replay routing.

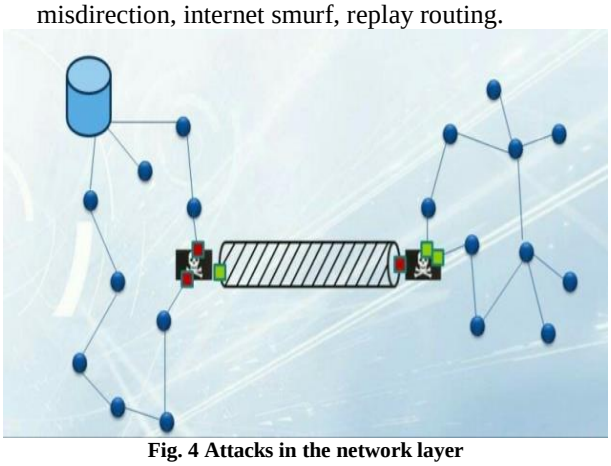

Fig. 4 Attacks in the network layer

d) **Transport layer:** Attacks are de-synchronization and flooding.

e) **Application layer:** Path-based DoS, overwhelm a deluge.

IV. SECURITY SOLUTIONS

This section gives the possible protective measures against all the WSN security attacks and threats. These solutions play a major role in protecting WSN systems. Following are some of the important terms for WSN security;

A. Cryptography

Protecting the information and communication involved in the sensor networks by using codes is known as cryptography. It ensures that only the authorized party can read and process the information. The basic requirement to provide security services in WSNs is the selection of appropriate cryptographic methods for sensor nodes [7]. To obtain security in WSN, it is essential to perform various cryptographic operations like authentication, integrity, encryption, confidentiality and so on. The security protocol for sensor networks (SPIN) has two secure building blocks, which includes Sensor

Network Encryption Protocol (SNEP) and µTESLA. Sensor network encryption protocol concentrates on data confidentiality, two-party data authentication and data freshness, whereas µTESLA provides broadcast for the resource-restricted environment.

B. Secure data aggregation

WSNs are restricted in energy and bandwidth. To bring a significant effect on power conservation and bandwidth utilization, it is important to reduce the communication between sensor and base station. Aggregated sensor networks work for reducing these communications [8]. The intermediary nodes in aggregated sensor networks which are known as aggregators, are involved in the collection of raw information from sensor nodes and process it and give out only the result to the end-user. These kinds of operations really reduce the transmitted data content, and so it lasts for an overall lifetime [12]. The active adversary makes the sensor authorize false aggregated results, which are far more different from the actual results. The other techniques used for reducing communication and management overhead for sending a message are multicasting and broadcasting techniques. Appropriate authentication and encryption mechanisms must be used to ensure that only authorized group members receive multicasting and broadcasting communication.

C. Key management protocols

Key management is the most important technique that ensures the security of in-network services and their applications in WSN. The main aim of key management protocols is to introduce keys among the sensor nodes in a secured and reliable manner. Key management protocols are distributed and centralized on the basis of the underlying network structure. There will be only one entity in a centralized key that controls the generation, regeneration and distribution of keys. This kind of entity is known as the Key Distribution Center (KDC). Key management protocols include four different kinds of keys [11], they are;

a) Individual key: It is a unique key in a sensor node that is shared in the base station of WSN. It provides individual authentication and secure communication assurance.

b) Pairwise key: It is the keys of sensor nodes that are shared with the neighbouring nodes. Therefore the storage of keys depends on the number of its neighbours.

c) Cluster key: An elected cluster head in WSN generates the cluster key. And such keys are shared with the neighbours. They are used in local broadcast packet encryption.

d) Group key: The encryption process for messages that need to be broadcast to the entire group is done by the group keys. There will be only one group key for the whole WSN network, which functions as a whole network.

D. Secure routing

Data integrity, authentication and availability of messages are ensured by the secure routing protocol. These protocols play a vital role in the acceptance and use of the sensor networks in many applications [11]. Insecure routing technique, the threats and attacks in WSN are protected by the security attributes.

E. Trust management system

Trust in the behaviour of the elements of the network is the main aspect of WSN. The trust management systems are mainly designed and prepared for working against issues like autonomy, decentralization and initialization that are found in WSN environments [13]. The cryptographic functions are used to compute the trust value of nodes in WSN.

V. CONCLUSION

The Wireless Sensor Networks are emerging as a promising technology in many communicating applications. However, there are many security issues that affect the confidentiality, integrity, authentication and availability of information to the users. Current researches and studies in providing security to the WSN have made the security attacks a little dull. In this paper, we presented both security issues and solutions for such issues. On the basis of our observation, we encourage the need for a strong security framework that controls all the attacks and threats in Wireless Sensor Networks.

REFERENCES

[1] Youssef charfi, Naoki wakamiya and Masayuki Murata., Challenging issues in visual sensor networks., Japan Society for the promotion of science.

[2] Tanveer Zia and Albert zomaya, ., Security issues in wireless sensor networks., international conference on systems and networks communication, (2006).

[3] Muawia Abdelmagid Elsadig., Security issues and challenges in wireless sensor networks., international journal of advanced trends in computer science and engineering, (2019).

[4] Mahfuzulhoq Chowdhury, Mdfazlul Kader., Security issues in wireless sensor networks - a survey., (2013).

[5] Mohamed Lamine Messai., Classification of attacks in wireless sensor networks., an international congress on telecommunication and applications, (2014).

[6] S.Nithya and Dr C.Gomathy., An investigation on security attacks in wireless sensor networks., international journal of pure and applied mathematics, 119 (2018).

[7] Madhumita panda., Security in wireless sensor networks using cryptographic techniques., American journal of engineering research, 3(1) (2014).

[8] Yingpeng Sang and Hong Shen., Secure data aggregation in wireless sensor networks, IEEE, international conference on parallel and distributed computing, (2006).

[9] Ms Poonam Barua and Mr Sanjeev Indora., Overview of security threats in wireless sensor networks, International journal of computer science and mobile computing, IJCSMC 2(7) (2013).

[10] Baojiang Cui, Ziyue Wang and Bing Zhao., Enhanced key management protocols for wireless sensor networks", mobile information systems, article id 627548, (2015).

[11] M.Nikijoo, A.S.Tehrani and P.Kumarawadu., secure routing in sensor networks, IEEE (2009) 978 – 981.

[12] D.Djenouri, L.Khelladi and A.Nahjiib Badache., a survey of security issues in mobile ad. hoc and sensor networks., IEEE communications survey and tutorials, 7(4) (2005).

[13] Y.Sun, Z.Han and K.J.Payliu., defence of trust management vulnerabilities in distributed network., IEEE communications magazine, (2008) 112-119.

[14] X.Chan, K.Makki K.Yen and N.Pissinou.,Sensor network security – a survey., IEEE communications survey and tutorials, 11(2) second quarter (2009) 52-73.

[15] G.Bianchi., A comparative study of the various security approaches used in wireless sensor networks., International journal of advanced science and technology, 17(2010) 31-44.

[16] T.A.Zia., A security framework for wireless sensor networks, http://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pd6, 2008.