IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 1, January 2020

Security Issues and Challenges in Wireless Sensor Networks: A Review

Mr. S. Hendry Leo Kanickam[1], J. Angel[2]

Assistant Professor, Department of Information Technology, St. Joseph's College Tiruchirappalli, India[1]

M.Sc., IT Student, Department of Information Technology, St. Joseph's College Tiruchirappalli, India[2]

Abstract: Wireless sensor network is the rising technology for sensing and performing the various tasks. Sensors are small device having memory, power and processing chip that makes it processing device. These WSNs have various purposes in many fields like Healthcare, industry, military, smart homes, etc.. WSNs have more advantages over wired networks. These systems are probably going to be made out of hundreds, and a large number of modest sensor nodes, working independently. Though there are several advantages of wireless networks, they are prone to security issues. Security became a major concern for wireless sensor networks because of the wider application. So, this paper addresses the security issues and challenges of WSNs in various layers of the communication protocols.

Keywords: Wireless Sensor Network (WSN), Network Security, Attacks and Challenges, Security Mechanism

I. INTRODUCTION

Today Internet has proved to be one of the effective pieces of day to day life. It's changed the way people live, work, play and learn. A Sensor Networks is a set of sensors with features like inexpensive, low power, self-organize and cooperative data processing and also, they possess advantages with various applications in real time. The sensor network made of a group of distributed sensors with sensing computation and for monitoring physical or surrounding conditions and transmitting their data to a base station via the network. The appealing features of the sensor network attracted many researchers to work on different issues relating to these kinds of networks. While the routing strategies and the Sampling of the Wireless Sensor are becoming much preferred, the security issues still need to be addressed extensively. WSNs used for mission-critical uses such as military surveillance or medical applications.

Where several low-cost nodes are connected to the human body to collect data and are moved regularly to a sink node for further processing. Sink node is also often designed to function as gateways to transfer data to cloud-residing e-Health systems. Moreover, despite their relatively low-cost approaches, WSNs are attracting rapid worldwide attention to a range of real-world challenges. Many other advantageous factors of using WSNs are self-organizing, self-healing, providing complex network topology to cope with node malfunction and failures, mobility of deployed nodes, unattended service, ability to withstand bad environmental conditions, flexibility of nodes, scalability, during deployment and after deployment and ease of use. A nodes or distension's ability to discover various compromised nodes enable them to do something too disregarding network reconfiguration to remove the danger.

- **Types of Network**

There are two main Network forms i.e. wired and wireless Network

a) **Wired Networks*:*** Wired network is those networks in which computer devices attached with each with help of wire. The wire is used as medium of communication for transmitting One-point data of the network to other point of the network.

b) **Wireless Networks*:*** A Network where, without any cable, computer devices Communicate between themselves. When a computer device wants to communicate with another device, the destination device must lay within the radio range of each other Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation.

II. LITERATURE SURVEY

Many researchers proposed anti-attack mechanism. The new security research on WSNs issues, threats and approaches that have been discussed are as follows: An attempt was made to explore the security mechanism commonly used to manage such attacks and also explain the classification of attacks in the network of wireless sensors.(Vikash Kumar,

DOI 10.17148/IJARCCE.2020.9140

Anshu Jain and PN Barwal) [1].In a WBAN, the current major security criteria and risks to DoS are outlined. This offered an exhaustive description for a WBAN of existing security protocols. Further work needed to implement and introduce new levels of security. The security nodes for a WBAN are AES-CTR, AESCBC-MAC and AES-CCM (Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo)[5]. Wireless Sensor networks pose delightful challenges for the distributed control application. In light of new technical possibilities, we need to apply relevant techniques and metrics That is, cheap nodes and limitations in the processing and sensing i.e. energy constraints. Visualization and novel debugging technologies designed for new sensor network challenges will be of great help in testing and maintaining new algorithms and applications.(B. Sangeetha)[2]. The attacks and their classification in WSNs were suggested and the protection mechanism was also studied as an attempt. This survey shows the cycle of security and Makes the network even bigger more secure. (Dr. G Padmavathi, Mrs. D Shanmugam Priya) [6]. There were many suggested authentication schemes to prevent Stop fake injection attacks in sensor network. By implementing one of the schemes on the Tiny OS-based Mica 2 motes, they demonstrated the feasibility of using their schemes on resource-restricted sensor nodes. (S. Zhu et al) [15].

III. RESEARCH METHODOLOGY

1. Why Used Wireless Networks?

Wireless networks are network of computers utilizing Wireless connection of data between network nodes.[1]Wireless networking is a means by which home Telecommunications networks and services stop the expensive process of installing Cables in, or as, a building link between different locations of equipment.[2] Networks are generally implemented and controlled via radio communication, this is accomplished on the physical level of the OSI model network structure.[3]Wireless Networks include mobile networks, Local Wireless (WLANs), Wireless Sensor (WSNs), satellite communications networks and land microwave networks.

Fig. 1 Communications in Wireless Networks

1.1. Wireless ad-hoc Network

An ad hoc Networks consists of a series of nodes the interacts without each other having to a pre-established networking infrastructure via wireless connections. It originated from the uses of battlefield communication, where networks of infrastructure are often impossible. There are many potential applications of a wireless the network is ad hoc because of its edibility in implementation. For example, in an emergency caused by disasters like an earthquake or floods, it can be used as a communication network for a rescue team where infrastructure might have been damaged.

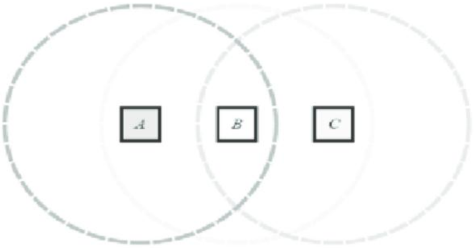

Fig.2 Simple Ad-Hoc Networks

1.2. Manet

Mobile hosts are creating an ad hoc network. Some of those centralized hosts are willing to move on neighboring packets. All nodes can move and can be arbitrarily connected dynamically. The tasks for network management and

DOI 10.17148/IJARCCE.2020.9140

control are Shared all terminals themselves. Some are in this type of networks, some terminal pairs may not be could communicate with each other explicitly, and have to respond to some other terminals in order to deliver the messages to their destinations.

1.3. Wireless Sensor Network

A) **WSN Architecture:** In a typical WSN we see following components of the network

i) **Sensor nodes (Field devices)** – Each sensor network node typically has multiple parts, an internal antenna transceiver ratio, An Electronic Microcontroller sensor and energy source interface circuit, Typically a battery or built-in battery energy source recovery.

ii) **Gateways or Access points** – A Gateway allows contact between host and field devices.

iii) **Network Manager** – Network manager is in charge scheduling the network configuration of base stations as one or more valued components of WSN to a lot more resources of distinguished components of WSN to a lot more resources for energy and communication computing. Most methods like satellite mobile phone networks using high-power radio modems with wi-fi links to the outside world.

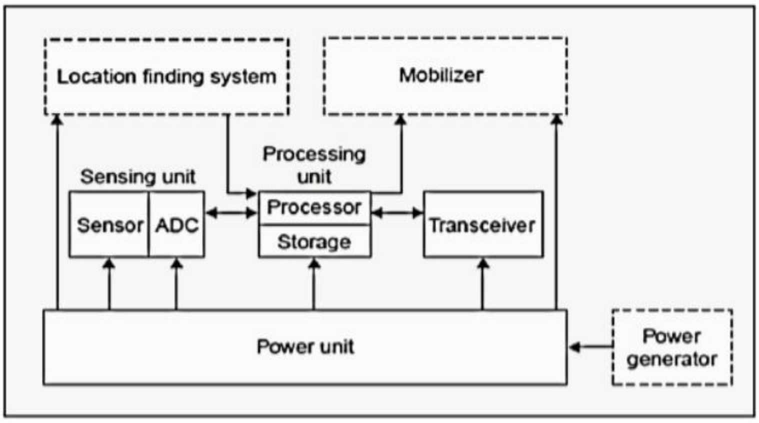

Fig.3 Power unit Flow Diagram

B) **Communication Protocol:** Wireless Sensor Networks employ complex infrastructure such as architecture with wired network. The following are the characteristics and behavior of each of their layers:

i) **Physical layer:** The aim of physical layer is to increase reliability by decreasing path less impact and shadowing. This layer is reliable for acknowledged communication, data rate, modulation, data encryption, signal detection and frequency generation.

ii) **Data link layer:** The purpose of link layer is to communicate between two nodes. It is this layer that is responsible for detecting errors and multiplexing. In addition, during network installation and maintenance to build stable key.

iii) **Network layer:** In addition, stable key development during network deployment and maintenance. Some scientists proposed using public key cryptography [4,13] and safe distribution of code [10] as possibly as possible. Network layer is aimed at this layer provides for routing, providing efficient routing technique, node to head of cluster and vice versa.

iv) **Transport layer:** In the outside networks, i.e. The internet-connected sensor network can use transportation layer setup communication, but in WNS, this is the most difficult issue.

v) **Application layer:** Use of application layer to view ultimate yield by guaranteeing low to lower layers of smooth details. This layer is responsible for collecting, handling and analyzing the data by using the application software to achieve accurate consequences.

C) **Security Needs of WNSs:** The main reason for security services in WSNs is to worry about the sequence of attacks and abuse resources. In WSNs the security needs include: [17]

1) **Data Confidentiality:** Confidentiality of Data is also known as data privacy. Because nodes are sometimes used to handle sensitive information, there are also a set of rules that have the limits on accessing the data.

DOI 10.17148/IJARCCE.2020.9140

Confidentiality is defined to prevent the data from entering the wrong or unauthorized sensor node. The specifics are not to fall into unintended hands, the knowledge of the community sensor, so that the identities of the sensor and the community keys are expected to be encrypted to a certain degree to protect next to attacks on traffic analysis.

i) There has to be one change to the Sensor Data for transit. It's the guarantee that the information during the contact process is trustworthy and reliable. For WSNs the credibility issues have the following requirements malicious node inserting False information in the WSNs."

ii) With poor wireless channel conditions, data loss is triggered.

iii) The network nodes should only have access to keys and only one delegated You should be allowed to change base station the keys. This would effectively prevent unauthorized nodes from gaining knowledge of the keys used, and would avoid notifications from external sources.

2) **Data Authentication:** Confirmation by identifying its source, guarantees the unwavering consistency of the message. Assaults in WSNs don't just include the modification of the bundles; enemies can also infuse extra fake packages. The personality of senders and collectors was checked in the validation of the information. Verification of knowledge is achieved by means of symmetrical or deviated components where hubs provide mystery keys to submit and accept.

3) **Data freshness:** Although honesty and confidentiality are ensured, we must ensure the freshness of the data. If the design uses a common key strategy the necessity for freshness is very relevant. With each message the counter is monotonically increased and the old counter value messages are rejected. According to the literature we have two forms of freshness: weak freshness carries no delay but offers partial and strong freshness gives estimate of delay and offers a complete order.

4) **Robustness and Survivability:** The sensor networks should be strong enough to withstand the attacks on security, and even if the attack is successful, the effect should be much less. A node's vulnerability should not infringe the security of the entire network.

5) **Access Control:** To maintain validity, access control requires the ability to distinguish users who access wireless sensor networks. Access control defines which system resources can be accessed, and how these resources can be abused.

6) **Secure Localization:** Sometimes, "the reliability of a sensor system depends on its ability to find every sensor in the system precisely. "A sensor system designed to identify deficiencies would need accurate area data to identify the region of a deficiency. "Safe Range-Independent Localization" is depicted in Sherlock." Its peculiarity is its decentralized, autonomous existence.

IV. SECURITY THREATS AND ISSUES

Due to the medium nature of the broadcast of medium wireless sensor networks, security attacks are vulnerable .More WSNs are also vulnerable, as nodes are often Located in a hostile or dangerous environment where physically vulnerable. Attacks are generally classed as active attacks and passive attacks.

A. Passive Attacks

Monitoring and listening by unauthorized threats to the communication channel is known as a passive attack. The Privacy Attacks are passive in nature. Some of the more famous anti-sensor privacy attacks [8] are: Monitor and Eavesdropping, Traffic Analysis, Camouflage Adversaries.

i) **Monitor and Eavesdropping:** This is the most frequent Privacy Attack. By snooping the data, the opponent could easily discover the contents of the communication

ii) **Traffic Analysis:** Even if the transmitted messages are encrypted, a high-possibility analysis of the communication patterns sensor activities will theoretically expose sufficient Data allowing an attacker to inflict sensor network malicious harm.

iii) **Camouflage Adversaries:** The nodes to hide in the sensor network can be inserted or compromised; After that these nodes will copy to receive the packets as a regular node, then misroute the packets and perform a privacy analysis.

B. Active Attacks

The unauthorized attackers track, listen to, and alter the communication channel data stream are known as active attack. The attacks below are real in nature. Routing Sensor Network Attacks, Subversion Node Failure System Outage, Physical Attacks, Signal Corruption False Terminal, Node Replication Attacks, Active Information Collection, etc.

DOI 10.17148/IJARCCE.2020.9140

C. Physical Attacks

Unlike many other above attacks, physical attacks permanently destroy sensors and Losses for this are permanent. For example, attackers are able to Extracting cryptographic secrets; manipulate the associated circuitry, Update or disable Sensor programming with malicious sensors managed by an attacker

V. SECURITY CHALLENGES IN WSN

The complexity of large wireless networks with ad-hoc sensors poses significant challenges in the design of protection schemes.

A. Wireless Medium: Inherently, as its broadcast nature makes eavesdropping easy, the wireless media is less safe. An intruder can intercept quickly, modify, or replay any transmission. The wireless medium lets an attacker intercept legitimate packets easily and inject false ones easily. While this issue is not specific to sensor networks, existing approaches have to be modified to operate efficiently on sensor networks.

B. Ad-Hoc Deployment: The ad-hoc design of the sensor networks means that there is no statically definable structure. Nodes can be deployed Use the Airdrop so prior to deployment nothing is known about the topology. Because the network must help nodes that may fail or be replaced configuration of itself. In this dynamic environment security schemes need to be able to operate.

C. Hostile Environment: The next risk factor is the hostile environment where sensor nodes operate. Motes faces the risk of attackers killing or capturing them. The intensely hostile climate provides the security researchers with a significant challenge.

D. Immense Scale: The proposed size of sensor networks presents a major challenge to the safety mechanisms. The simple networking of tens to hundreds of thousands of nodes has proven to be a significant challenge.

VI. SECURITY SOLUTION IN WSN

A. Directional Antennas

A wireless sensor network's physical layer is responsible for bit-stream transmission / reception over wireless communication networks, performing a series of tasks including selection and generation of carrier frequencies, signal detection, modulation, or data encryption. Antenna devices which basically turn electrical power into electromagnetic waves, or vice versa, play a central role in this context. To be used in WSN nodes, directional antennas must have four essential functionalities: They must be lightweight, reasonably priced, low power consumption and capable of operating in licensed frequency bands. Directional antennas can reduce or even eliminate the risks associated with certain types of security attacks on WSNs due to their particular radiation pattern that can materialize through adjacent or malicious node localization mechanisms or may drastically reduce the areas from which the attack can take place. Eavesdropping, jamming, attacking Sybil and attacking the wormhole, however similar countermeasures may reduce the risk of traffic analysis man or node catch in the middle assault

VII. CONCLUSION

As WSN continues to evolve and is commonly used in several high-impact applications, the need for the safety mechanisms is becoming very important. Wireless Sensor Network security is essential for the acceptance and usage of sensor networks. WSNs in manufacturing, product in particular will not get acceptance unless the network has full proof of protection. The node nature in WSNs causes limitations like limited energy. Such limitations establish WSNs that are so disruptive to traditional Ad Hoc broadband networks. In WSNs specific methods and protocols were developed for use. All of the security hazards mentioned, including the Hello flood attack, Wormhole attack, Sybil attack, Sinkhole attack, offer one usual goal of compromising the integrity of the network they are attacking. Since the various dangers and the importance of data exist confidentially, the protection of WSNs become a major subject, although in the past there has been a little concentration on security of WSNs the paper discusses the attacks and their classifications in WSNs, and there was also an attempt to explore the security mechanism commonly used to manage those attacks. It also briefly examines the challenges facing Wireless Sensor Networks.

DOI 10.17148/IJARCCE.2020.9140

REFERENCES

[1]. Vikash Kumar, Anshul Jain, PN Barwal, "Wireless Sensor Networks". International Journal of Information and Computation Technology, Vol. 4 .pp.859-868, 2014.

[2]. B. Sangeetha, "Wireless Sensor Networks: Issues Challenges and Survey of Solutions", International Journal for Scientific Research and Development, Vol. 2, May 2014.

[3]. Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. IEEE International conference on Space Science and Communication,1-3 July 2013.

[4]. L. Jialing. Valois , F; Dohler M , Min You Wu, "Optimized Data Aggregation in WSNs using Adaptive ARMA, "Sensor Technologies and Applications (SENSORCOMM) 2010 Fourth International Conference on, pp. 115- 120 , 18- 25 July 2010.

[5]. Shahnaz Saleem, Sana Ullah, Hycong Seon Yoo, "On the security issues in Wireless Body Area Networks" International Journal of Digital Content Technology and its Application, Sep 2009.

[6]. Douceur, J. (2002) the sybil attack. International Workshop on Peer-to-Peer Systems (IPTPS'02).

[7]. Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced CommunicationTechnology (ICACT), Page(s):6, year 2006

[8]. Franklin, M. Galil, Z. and Yung, M. (2000). Eavesdropping games: a graph-theoretic approach to privacy in distributed systems," J. ACM, 47, 225–243.

[9]. Karlof, C and Wagner, D. (2003). Secure routing in Wireless Sensor Networks: Attacks and Countermeasures, Adhoc networks, 293395.

[10]. Kurak, C and McHugh, J. (1992). A Cautionary Note on Image Downgrading in Computer Security Applications. Proceedings of the eighth Computer Security Applications Conference. 153-159.

[11]. Murthy, C. R. In addition, Manoj, B. S. (2004). Transport layer and security protocols for ad hoc wireless networks. Ad Hoc Wireless Networks - Architectures and Protocols.

[12]. Newsome, J. Shi, E. Song, D, and Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses. Proc. of the third international symposium on Information processing in sensor networks, 259 – 268.

[13]. Parno, B. Perrig, A. and Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. In Proceedings of IEEE Symposium on Security and Privacy.

[14]. Pathan, A S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S. (2006). A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks. IEEE ICNEWS

DOI 10.17148/IJARCCE.2020.9140