IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

WSN – An Emerging Technology and its Security Meaures

Shafiqul Abidin

Department of Information Technology, HMRITM (GGSIP University), Delhi, India

Available online at: www.ijcseonline.org

Accepted: 19/Sept/2018, Published: 30/Sept/2018

***Abstract*—** Wireless Sensor Network (WSN) is one of the merging network technologies. It is an extensively distributed network equipped with low powered and lightweight wireless sensor nodes. WSN are being deployed to monitor system and environment. WSN are being used in health sectors, military operations, automation industries, traffic monitoring, oil refineries etc. But with the emerging applications, WSN is prone to attacks and threats. These attacks and threats must be studied thoroughly in order to counter them. Today security issues are the major challenges faced by WSN. The deployment of wireless sensor nodes in hostile environments makes them the subject of lethal attacks, also due to the limitations of resources processing capability, power consumption & communication range WSN are vulnerable to many types of threats/attacks. There are serious consequences if security of WSN gets compromised by any means such as information theft, lack of privacy, etc. Thus it must be our utmost priority to save WSNs from malicious attacks. In this study we have highlighted the various fatal attacks that can destruct WSN with their impacts and consequences.

***Keywords*—**WSN, Network Security, Cryptography, Confidentiaity, Authenicity, Blackhole, Jammming.

I. INTRODUCTION

Wireless Sensor Networking (WSN) is an area where active research can be done using different kinds of algorithms, models, security and social factors [1]. WSN are being used widely in defence sectors. It is also helpful to monitor the process and track the locations of an object. A wireless sensor network (WSN) is equipped with autonomous sensors. These sensors are enough smart to measure and sense pressure, temperature, sound, light, moisture, etc. These sensing / measuring data can be transmitted via an interconnected network to processing centre / base station. This indicates the communication between two objects or bodies is being taken place without having any kind of physical connection between them i.e. wireless. A sensor is an object whose purpose or job is the detection of events or changes in its environment, and then providing a corresponding output. A sensor can also be said as a type of transducer. These sensors can produce different types of output. Basically we are using a technology where we can connect different nodes to each other in order to communicate through different channels (other than physical channel). Since this technology is extensively used, therefore, Security becomes a major cause of concern here. The security models we have are too traditional and cannot be used to serve the purpose of this latest technology. Sensors comprise unique characteristics and hence attackers have different ways to capture the control and aim at controlling those nodes and learn a new secret material to intercept or tamper messages. The networking architecture heavily depends on the environmental factors and the disclosure of these factors may be harmful for the security of information. There are differences which determine the security effectiveness like, difference between the nodes of sensor networks and nodes in normal condition networks in terms of their numbers, environmental conditions, topologies, memory, mobility etc. These differences highly affect the data security for example, WNS might more prone to denial-of- service attacks [2]. Cryptography trustworthy and efficient method that uses symmetric keys for security designs. Here, we can assure secure data aggregation using this technique [3]. It is better to have a aggregation design for secure aggregation. We have to find out feasible and optimal recovery techniques to handle different threats and attacks.

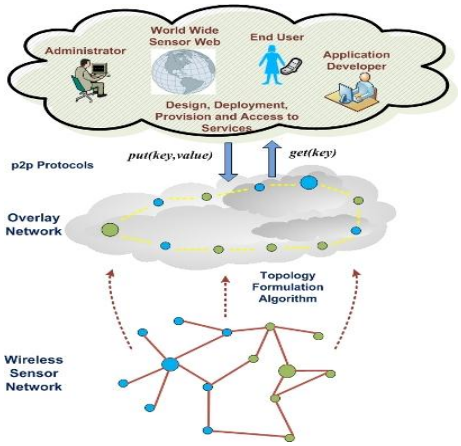

Figure 1. Schematic Representation of WSN

This article is divided into six sections. Section II is the Security Objective which tells the reasons for which the paper is written. Section III tells us about the Denial-Of-Service attack which is the most common attack in the WNS system. Section IV tells us about the next three attacks that are also often affect WNS namely Sybil, Wormhole and Blackhole/Sinkhole. Section V describes the another three attacks that are not extensively used, they are Hello World, Jamming and Selective Forwarding. Finally section VI concludes our paper [4].

II. OBJECTIVES OF SECURITY

The prominent security objectives are being discussed as follows.

A. Confidentiality

This is one of the most important aspects we need to ensure. The data which is being transmitted between nodes should be confidential that is, privacy should be there. This could be done using encryption. The source can encrypt the data and the sink can decrypt the data to obtain the information.

B. Authnticity

The data should be authentic which means when the packet is received, it should be verified that it comes from a trusted source. If authentication is not there, the attackers can tamper the message anywhere in between due to which wrong message would be transmitted to the sink [5].

C. Availibility

WSN's services should be available when it is requested by the user. Attackers use malicious programs causing DOS and performance is reduced. This causes network failure and results could be catastrophic.

D. Integrity

The data which is received should be integral which means the sequence of the messages received should be same as it was sent. Attackers can interrupt and change the messages sending a wrong information to the sink [6].

E. Data Freshness

This ensures that the data received at the sink is fresh, i.e. the information received is that latest and no earlier messages are being resent to the sink again. This causes confusion in networking and may be a victim of an attacker. This problem can be solved using Timestamp to monitor the messages time.

F. Access Control

This controls over the users who are not allowed to use the services.

III. DENIAL- OF –SERVICE (DOS) ATTACK

Here, malicious programs are used to attack the network .this results in denial of service that is it refuses to operate as per user's requirements for instance, not accessing users use those services which they were allowed to use before [7]. This attacks is done by sending unnecessary extra packets .It reduces the ability of the network to operate its functions properly. It explicitly prevents the user who is legitimate to use the services. It overloads the system with requests so that it becomes difficult for the network to handle the traffic. This reduces the overall performance of WSN. This attack is done in 4 different layers. First one being Physical layer, this is the basic layer and is reliable for encryption, detection of signals, modulation. The types of attacks which are done in this layer are Jamming (in which the frequencies are jammed) and Tampering (easy access to nodes). We can tackle these attacks by using spread spectrum and priority messages for Jamming and Tamper-proof or hiding against Tampering. Second is Link layer. The job of this layer is to assure the connection and exchange of information between the nodes. This recognizes the error and Tiny Sec is used for its protection .Several kind of attacks can be done like collision (here retransmission takes place of packets), unfairness and exhaustion (Repeated collision leads to power supply exhaustion of nodes). Code can be error corrected to avoid collision. Smaller frames can be used for unfairness and rate limit is a defense for Exhaustion attack. Third layer is Network layer which is layer is highly prone to attacks. Different Protocols is used to route the data from node to different locations. Blackholes attack can be defended by monitoring, authorization and checking redundancy. Another kind of kind possible is routing the information which is spoofed and forwarding selectively and this can be defended by monitoring and authorization and Egress filtering. Misdirection is also an attack which misdirects data to wrong location can be solved by authentication. Last layer is the Transport Layer and this is used for the local network connected to the Internet. But this is a difficult task. A kind of attack possible in this layer is Flooding Maliciously and this attack can be counteracted by Client puzzles and limitation of rate. The attacks shown in all the different layers can be prevented by Rigid authentication, Traffic identification and pushback mechanisms.

IV. SYBIL, WORMHOLE & BLACKHOLE ATTACKS

Sybil attack takes place in routing layer .This is an attack in where there is a node which displays the identities of more than one node. This attack is highly prone to the peer-to-peer networks [8]. The basic purpose of attack is to degrade the

integrity (data), use multiple redundancies, and lower the utilization of resources and security. The memory is filled unnecessarily with useless data. The name "sybil" actually came from a book as it once help in diagnosing a woman who was suffering from multiple identity disorder so we can say similarly the nodes possess multiple identity. The attacks are more prone to storage distribution systems, aggregating and allocation of resources. Encryption is a way to prevent these attacks. Validation techniques are also an alternative to tackle this attack. Individuality should be legal whether it is direct or indirect. To counter attack, first of all trusted certification should be there. Although, this is good method to provide uniqueness however it proves to be costly in case of large scales systems. It is also proposed that IP addresses can also be tested for various autonomous systems. This might prevent the attack but may also affect the performance of the system. Various algorithms are also proposed for cryptographic keys to defend the attack. This can be certified showing its physical traits but here also, applying to a large systems is a challenge.

Wormhole attack takes place while transmission of data and occurs in routing layer. Messages are tunnelled by maliciously programmed nodes and then it is retransmitted to the receiver part which exploits the routing conditions. Here, the data passes through the attacker and then does not reach to its respective place or node/location where it was supposed to, else is sent to the other place in the networking system and then it reaches its destination via attackers' locations .This is amongst widely used attack and can be used at any time of transmission phase [9]. If nodes are very far away then it is more prone to this attack. This can easily be used along with Sybil attack. Here, Encryption technique will not work to counteract the attack. This attack gives a straight challenge to the cryptographic protection and confuses the protocols. To tackle this, private channel can be used to transmit the message. A four-way handshaking technique is also an alternative. Nodes can have their own direction antennas to provide proper direction. The distances between should be monitored carefully so that there is least scope for a worm hole attack.

Black hole / Sink hole also affects routing layer of WSN. Malicious node imitates as blackhole and aims at drawing all the data traffic through the compromising node creating a sinkhole with opponent or adversary in centre. In other words hostile node advertises itself in between the zero cost routes. Here, the blackhole is referred to the node which is maliciously programmed and inserted in between the source/generation and the sink/destination. The node or the attacker in between receives the packets and is able to do any kind of misuse with the packets like tampering and then sending it to the destination or dropping packets selectively. WSN is highly vulnerable to this attack as the flow of packets is towards the sink(single point of failure)In other words we can say it can packets are magnetic in the networking system. This is difficult to prevent and detection is rare. It can be counter act with the help of typical mechanism which will guide the nose so that the relevant node will not listen to the unethical information from malicious node which leads to sink hole. In other ways making the node aware of the entire network system can reduce this attack. Also the use of some protocols like cryptography methods with key can be employed to ensure security of route with end to end acknowledgements contains latency information and reliability [10].

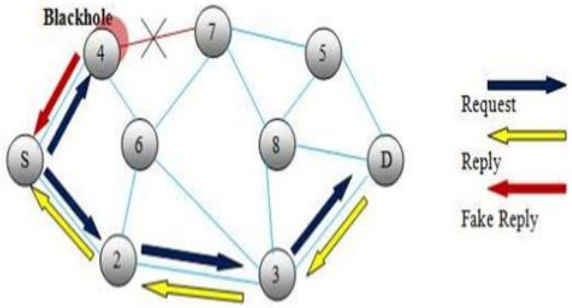

Figure 2. Blackhole Attack

V. HELLO FLOOD ATTACK / JAMMING AND SELECTIVE FORWARDING

Hello Flood Attack attacks the sensor nodes by introducing a new type of attacker named as Hello packets. Hello packets are smaller in size as compared to data packets. The hello flood has higher probability of reaching receiver than that of data packets over weak links. Hello packets guarantee no bidirectional communication and are broadcasted without any acknowledgement. These packets are sent in a huge area having high processing power to numerous sensors so that a number of nodes far away can sense it as the parent node [11]. This assumption of parent node may sometimes be false; an attacker broadcasting routing and other information providing large transmission power convinces every node present in the network that the adversary resides in neighbors. For example, a foe advertising a very high quality route to the base station to every node present in the network could makes a large number of nodes to attempt follow this route, but those node far away from the foe would be sending data or packets into void. Hello message gets broadcasted into large are making node to sense that the attacker is their neighbour that is available in communication range and they all respond to Hello message in result wasting their energy. Even if the node realizes that it has made link to the adversary then also it is left with fewer options as all it neighbors are sending packets to adversary as well. Thus the network is left in a state of confusion. Here, the packets are when being transmitted passes through the attacker and are

victim packets and these packets are replaced by the fake packets while transmitting the data to the base station without letting anyone knowing about it. This is very easy to attack and considered as the one of the main attack of network layer of the wireless sensors networks [12]. "Identity Verification Protocol" can be used to counteract this attack. It permits bi-directionally of a link with encrypted echo back mechanism even before taking some action based on the note received over that link. It affects the routing layer of WSN. To prevent this, Blocking Methods might be used.

A. Jamming

Jamming attack acts on the physical layer of the WSN. Jamming attacks basically interfere with the transmission and reception which takes place between nodes via wireless medium using radio frequencies signal. Attacker here tries to broadcast the signal of same frequency band or frequency sub band as that of transmitter and causes interference. There are various types of jammers that deliberately inject the false data in the process of communication which affects the data transmission between two nodes. Also it affects the WSN performance as it leads to overutilization of resources like memory, battery, etc. There are several types of jammers:-

- Constant Jammer
- Deceptive Jammer
- Random Jammer
- Reactive Jammer**.**

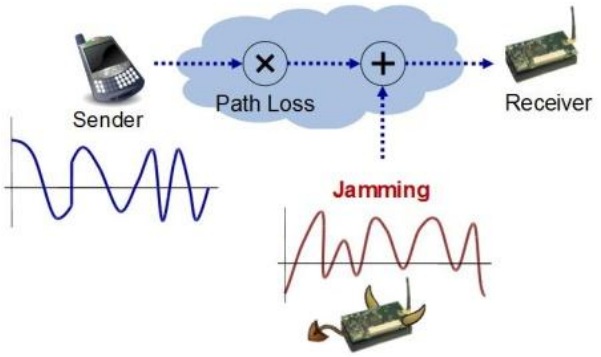

Figure 3. Jamming

Constant Jammer: The function of the constant jammer is to continuously emit a radio signal. , Either waveform generator or an ordinary wireless device is used for its execution. It continuously sends radio signals in the form of random bits to the channel [12]. The constant jammer opposes the hold of legitimate sources from getting the control or hold of the channel and sending packets.

Deceptive Jammer: The deceptive jammer continuously sends out regular packets on the channel instead of sending random bits additionally without any gap between the packets. As a result, it deceives an ordinary Communicator into believing that there a legitimate packet and can be conned to remain in receive state.

Random Jammer: It does not send out radio signal continuously instead a random jammer alternates between jamming and sleeping. After turning off its radio signal it gets into sleeping mode. Then it resumes its jamming after sleeping for some time. Jamming phase may either be deceptive or constant. Random jammer takes energy conservation into consideration as it does not have unlimited power supply.

Reactive Jammer: All aforementioned jammers are active jammers as they keep the channel busy at all times. This jammer is also called reactive jammer as is remains quite until the channel is idle mostly and comes into action as soon as it senses there is traffic or transmission in the channel. Among all Reactive Jammer is very harder to detect.

We can evade jamming attack using "Channel surfing". The motivation behind this technique is frequency hopping modulation. In channel surfing if a node senses interference it simply changes its current channel to a new channel in order to avoid interference. Problem with this technique is that it is suitable only for two nodes system. Also the channel switching leads to unreliable co-ordination of channel frequencies. We can overcome this problem if we only use the jamming regions to shift to the new channel.

B. Selective Forwarding / Grey Hole

Attacked in routine layer, nodes which are maliciously programmed cause some loss of data in between transmission. In other the packets are selectively dropped and data is thrown. This attack may show catastrophic results as the information may not be received properly at the end of receiver or we may have no output shown at all. This attack needs may cause for concern. The solution for this attack can be multipath routing which can be a very effective solution here [13]. The messages can be sent through many different paths thereby decreasing the probability of loss of data as data is divided. In addition to that, the nodes can also be monitored by using watchdogs kind of stuffs to control the interception and loss of data. The neighbor node can monitor the packets being flowed and detect the selective forwarding attack and if it is detected, the packet can be resent to the destination node and send a message about the attack to the adjacent node. Another scheme can be used in cluster networks. Here, the no of packets sent and received must be same to solve the problem. Ad-hoc on-demand Distance

Vector (ADOV) gives a proposed routine algorithm to tackle this attack. It is divided into two phases, Counter –threshold and Query based. In the former the packet counter is used to detect the attacks and in the latter, it uses the information from the neighboring nodes to identify the source of attack or attacker. Here, we prefer to find out the adjacent node as it increases the probability of finding the attacker. Query of many nodes may lead to degrading of performance [14].

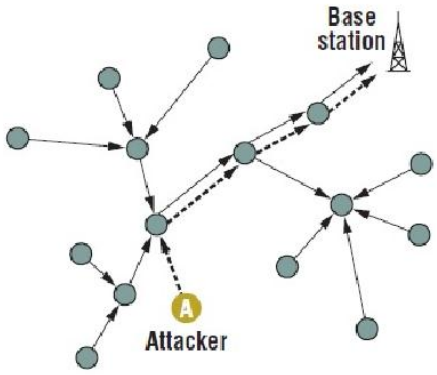

Figure 4. Selective Forwarding Attack

VI. CONCLUSION AND FUTURE SCOPE

As Wireless system are becoming an integral part of our lives , therefore, this makes this field more prone to attacks, so here security is a major cause of concern . This paper is summarized to know the various kinds of attacks possible in the field of WSN. An attempt has been made to explore the mechanisms used to handle such kind of attacks and to improve security. Most of the security attacks are often done by inserting the false information between the transmission or inserting the malicious nodes deceiving the networking system. This could be prevented by strongly detecting the false objects in the system. Integrity is one of main challenges in WSN. Security goals enables us to think somewhat like the attackers, this can help us to develop the better networks and detection systems for intervention in future. Also if new methods are found, researchers must also stick to security essentials like firewalls, encryption, antivirus etc. Few limitations that usually occur in such processes has also been discussed and it is hoped that the researchers in future can have a good overview and hopefully will generate a much efficient mechanisms to tackle these attacks and make the networking more robust, sensible and highly significant.

REFERENCES

[1] Al-Sakib Khan Pathan ,Hyung-Woo Lee, ChoongSeon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, Proc. ICACT 2006, Volume 1, 20-22 Feb, 2006, pp. 1043-1048.

[2] N. Gura, A. Patel, et al. "Comparing elliptic curve cryptography and RSA on 8-bit CPUs." Cryptographic Hardware and Embedded Systems-CHES 2004, pp 925-943, 2004.

[3] Hung, X, L, et al. “An Energy-Efficient Secure Routing and Key Management Scheme for Mobile Sinks in Wireless Sensor Networks Using Deployment Knowledge,” Sensors, Vol 8. 2008, 7753-7782.

[4] L. Jialiang, 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] RobertSzewczyk, Joseph Polastre, Alan Mainwaring, and David Culler. Lessons from a sensor network expedition. In First European Workshop on Wireless Sensor Networks (EWSN 04), January 2004.

[6] Kalpana Sharma, M.K. Ghose, Deepak Kumar, Raja Peeyush Kumar Singh,Vikas Kumar Pandey. “A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks”. In IJAST, Vol 7, April 2010.

[7] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 - 36.

[8] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[9] Hu, Y.-c., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 - 1986.

[10] Sheela D. Naveen K,C and Mahadevan G, A non cryptographic method of sink hole attack detectionin wireless sensor networks, Recent Trends in Information Technology (ICRTIT), 2011 International Conference IEEE.

[11] Hamid, M. A., Rashid, M-O., and Hong, C. S., “Routing Security in Sensor Network: Hello Flood Attack and Defense”, to appear in IEEE ICNEWS 2006.

[12] Choong Seon Hong. "Security in wireless sensor networks: issues and challenges", 2006 8th International Conference Advanced Communication Technology, 2006.

[13] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, Wang Liangmin, “Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks’ pp 226-232, IEEE 2009.

[14] Ahmad Salehi, S., M.A. Razzaque, Parisa Naraei, and Ali Farrokhtala. "Security in Wireless Sensor Networks: Issues and challanges", 2013 IEEE International Conference on Space Science and Communication (IconSpace), 2013.

Authors Profile

Shafiqul Abidin is presently associated as Professor & Head – Department of Information Technology with HMR Institute of Technology & Management (Affiliated with Guru Gobind Singh Indraprastha University), Delhi, India. He has published many research papers in national / international journals of repute and conferences. Dr. Abidin has visited various countries for teaching and research purpose in their institutions for a period of more than five years.

