A Survey on the Issues of Security Challenges and Solutions of Attacks at different layers of WSN

[1]Akash Jeewan
[1]M.Tech. Student
Jeewanakash91@gmail.com

[2]Rashid Hussain
[2]Ph.D. (P)

[3]Hari Ram Tanwar
[3]Asst. Professor

Suresh Gyan Vihar University, Jaipur, India

Abstract

Wireless Sensor Network (WSN) is an emerging field where the deployment of WSN has been boosted by the continuous and significant advances of hardware manufacturing technologies. Environmental Monitoring, Industrial Sensing, Military, Ecological and Health are some of the different areas where the use of Wireless Sensor Network is applied. The movement of enemies on the battlefield or locating of personnel in buildings are often sensitively monitored by these applications. So the concern of security in various applications of WSN, a few applications mentioned above, has become the topmost priority. Various constraints such as low computation capability, small memory, limited energy resources and use of insecure wireless communication channels are some of the main disadvantages and security threat to WSN. Different types of security threats may be devised by the attackers to make

the WSN system unstable. So all these constraints make security a challenge in WSN. The paper gives a detailed review on security issues, attacks and various vulnerabilities in WSN.

Keywords- *Security, Solution, Threats, WSN Layers.*

I. INTRODUCTION

WSNs are composed of sensor nodes on huge scale having certain characteristics such as low power, computation, storage and communication capabilities. Hundreds or thousands of nodes comprises a WSN having power unit, a sensing unit, a processing unit and computation capabilities to monitor the real world environment [1]. Due to its diversified application areas it has emerged as a dominant technology in the current decade. There are many application areas of WSN such as battle field awareness, traffic monitoring system, etc where security of information is a very important issue [3]. Security has become a well established field for general purpose computing where security mechanisms address computing services and provide secure transaction. As we all know that how important security is any field but a very little work has been done for securing a WSN. If we study the features of a WSN we will come to know the limitations of current security mechanism. Several features such as low memory, low energy, low bandwidth for communication and large scale nodes make most of the current solutions available [9]. As the lifetime of a sensor node is confined by the battery life so consumption of power is set as the first priority in developing security solutions. As the networks of a sensor are deployed in a hostile environment they are prone to different types of malicious attacks and thus security has become extremely important. For the success of WSN applications security in WSN has to be increased efficiently. For example; In military, the sensed information needs to be kept confidential and authentic from outside intruders. On the other hand correct analysis of security requirements helps us to develop or implement the proper safeguards against security violations. As there are varieties of challenges in sensor networks so different types of security issues and possible remedies are discussed in this paper. Some of the challenges [10] faced while providing security are as follows:

First challenge: Some of the constraints should be taken in while designing any security solution such as

limited energy, limited power, limited memory and limited bandwidth.

Second challenge: The topology of WSN is dynamic and sensor nodes present may get damaged and other nodes can be placed whose nature can be unpredictable.

Third challenge: The overall cost of the deployment of WSN should be as low as possible.

II. THREATS AT DIFFERENT LAYERS OF WSN

Here we will discuss on the threats present at different layers and some common threats which may be present on more than one layer of WSN [7], [10].

A. Physical Layer

Characteristics of physical layer are frequency selection, carrier frequency generation, data encryption, etc. Some common attacks on this layer are as:

Jamming: It is a type of attack which is related with radio frequencies. The jamming source may be either very powerful or less powerful and may jam the network. It is one of the denial of service attacks in which the operation of the network is disrupted by adversaries by broadcasting a very high energy signal.

Tampering: When nodes are damaged physically it is called as tampering. In this the attacker may damage, replace and electronically interrogate the nodes to acquire information.

B. Data Link Layer

This layer is responsible for insuring interoperability amongst communication between node to node. As data is transmitted in open medium so its security is under attack.

Collision: When transmission between two nodes is done simultaneously at same frequency then collision occurs. Due to which checksum mismatch occurs at the receiving end.

Exhaustion: When transmission of large number of request to send packets is done over media then this attack occurs which leads to multiple collisions of packets.

Sybil Attack: It induces negative reinforcements which changes the message to a false one.

C. Network Layer

It helps to find the path for efficient routing mechanism.

Sinkhole attack: Attraction of traffic to a specific node is called sinkhole attack. The adversaries try to attract all traffic from a particular area.

Sybil Attack: The node present in the network possesses more than one identity to the network.

Wormhole Attack: A wormhole is a low latency link between two portions of the network over which an attacker replays network messages.

D. Transport Layer

End to end connection is managed at this layer. An attacker when strong may attack the layer.

Flooding attacks: The state information which are present at either end of the communication are maintained by the protocol are vulnerable to flooding attacks. TCP SYN is a well known flood attack in which the adversary continuously sends the connection requests and floods the network link at the targeted node.

De-synchronization attacks: Transmission of missed frames at one or both end points alerts the adversary to maintain a proper timing and stops the end points from exchanging any useful information.

III. SOLUTION AT DIFFERENT LAYERS OF WSN

A. *Physical Layer*

Jamming: Frequency hopping spread spectrum is a method of transmitting signals by rapidly switching a carrier among many frequency channels using pseudorandom sequence known to both transmitter and receiver. If the attacker is unable to follow the sequence of frequency then jamming is impossible.

Tampering: When the sensor nodes are accessed physically by someone the nodes vaporize their

memory contents and thus leakage of information is prevented. This is called self destruction.

A. *Data Link Layer*

Good encryption mechanism, authentication mechanism, and error correcting techniques are required to put defense against most of the link layer threats.

Collision: Error correcting codes is used to defend against collision but this is costly in terms of energy consumption.

Exhaustion: We can use TDM where each node is allotted a different time slot for transmission.

B. *Network Layer*

Worm hole attack: During selection of path if we check the bi-directional link then this attack can be defended. Location based protocols may help us to avoid this type of attack.

Sybil attack: In this layer effective defense mechanism against this attack is not available. The defense mechanism against this attack is present at the data link layer and it can be defended there only.

Sink hole attack: Geo-routing protocols are used for protection against sink hole attack. The traffic is routed through the physical location of the sink node making it difficult to create a sink hole.

C. *Transport Layer*

As flaws exist in the transport layer protocols so the issue of security is there at this layer.

Flooding attack: If limitation is put on the connections from a particular node then it can be defended. The limitation should be set carefully.

De-synchronization attacks: Authentication of packets including control fields communication between hosts is required to check this attack.

IV. SECURITY ISSUES

Intrusion Detection: In the case of WSN the problem of intrusion detection is very important [6]. Some analysis done on the network based on traditional approaches proved to be expensive in terms of energy consumption and memory. This detection is largely open to research. Many aspects can be obtained from this detection but due to constraints they are not concerned. Integration of this technique into a uniform hardware platform seems to be difficult because of cost and implementation constraints.

Secure Location Discovery: Sensors placed at certain locations play an important role in monitoring and target tracking. Without security an attacker may mislead the location and interrupt the operation of sensor networks and give false information.

Secure Localization: The sensors must notice the location from where it is collecting information for security purpose. Many routing protocols require exact location to provide protocol service.

Secure Routing: The routing protocols should be secure enough to route information from source to destination. The attributes considered for security are identity verification, topology structure restriction and base station decentralization.

Limited Memory: Memory capacity of sensors is small so executing larger programs need more memory.

Power Consumption: Sensor nodes require large amount of energy for selection of route and searching for nodes. But maximum energy is consumed in node verification, encryption, decryption, etc and this should be minimized.

V. RELATED WORK

A lot of work has been done at different layers of WSN to provide security. Several methods have been suggested to detect and tolerate false information. But all these have not been able to provide security from different attackers on large scale. Using radio transmission with the constraints of small size, low energy and low cost make WSN susceptible to denial-of-service attacks. Some standard routing protocols were designed which were applicable only to two parties and could not be used on a large scale. Certain

work has been done on intrusion detection and lightweight framework Lidea has been designed for WSN. Lidea is distributed architecture work in which neighbour nodes checks nearby nodes and together coordinate to detect intrusion successfully. Lidea can be used to defend against wormhole attacks.

VI. CONCLUSION

We have discussed on threats and their solutions at different layers of WSN. As we learnt security has become a great issue and needs to be controlled to a larger extent to allow transmission of data securely and efficiently. Many protocols designed have not taken security under consideration. Some of the salient features of WSN makes security a challenging task. This paper is summarized on the attacks on sensor layers and surveyed literatures on several important security issues.

REFERENCES

[1] Hiren Kumar Deva Sarma, Avijit Kar, "Security Threats in Wireless Sensor Networks", IEEE 2006.

[2] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004 pp. 38–43.

[3] Raymond D.R. Midkiff.S.F, "Denial of Service in Wireless Sensor Network: Attacks and Defenses", IEEE Pervasive Computing,Vol:7, Issue 1, PP: 74 –81, March 2008.

[4] I. F. Akyildiz W. Su, Y. Sankarasubramaniam, "A Survey on Sensor Networks," IEEE Commun.Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[5] Xiaojiang Du; Hsiano-Hwa Chen; " Security in wireless sensor networks", Wireless Communications, IEEE, Vol: 15, Issue 4,pp: 60 –66, Aug 2008.

[6] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006

[7]Fei Hu, Jim Ziobro, Jason Tillett, Neeraj and K. Sharma, Secure Wireless Sensor Networks: Problems and Solutions, internet draft

[8] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Netw., vol. 1,no. 2, pp. 293–315, sep 2000.

[9] William Stallings, Cryptography and Network Security Principles and Practices, Third Edition, Pearson Education. ISBN 81-7808-902-5.

[10] Chennakesavulu V., B. Dey and S Nandi, Securing Wireless Sensor Networks: Challenges in Different Layers and Possible Solutions, Proceedings of National Workshop on Trends in Advanced Computing NWTAC 2006, pp. 73-82.