ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 7, Issue 2, February 2018

A Brief Review on Security Attacks in Wireless Sensor Networks

Sreelakshmi T.R, Dr. Binu G.S

***Abstract*— Wireless sensor networks are application specific networks which differ from traditional ad-hoc networks for its sensing, nature of deployment of nodes and the communication paradigm. The limited resources in wireless sensor networks are always a key challenge for its security. This makes them impractical to directly apply the traditional security mechanisms as such. This paper provides a review on the security threats in wireless sensor networks, specially focusing on the routing layer where the routing mechanisms and data transmission protocols are significant .This provide research directions in more routing solutions for security attacks issues.**

***Index Terms*— Wireless sensor networks, sensor nodes, security goals, security attacks**

I. INTRODUCTION

Wireless sensor network is an infrastructure less network consist of hundreds and thousands of low-cost, low-power, multifunctional devices called sensor nodes that are small in size and can communicate over short distances [1]. These tiny sensor nodes consist of sensing, data processing, and communicating components that are proficient to monitor the real-world environment. The sensor node, sink node, the user node constitute the different elements of a sensor network. Sensor node is the foundation of the whole network. They are responsible for the perception of data, processing data, storage of data, transmission of data and forwarding of data to neighboring nodes in a cooperative manner. A sensor node monitors the network after deployment, detect any event of interest queried by the sink and generate a report. The reports are transmitted to the base station via multi-hop wireless channel. The BS processes the report and sends it to the external world through high quality wired or wireless links. Thus sink serves as gateway between external world and the WSN. The sensed information includes temperature, humidity, light condition, vehicle movement, pressure, mechanical pressure strength, the speed of the airflow direction and other characteristics. Sensor nodes (SNs) are generally static in nature while mobile nodes can be deployed based on the application requirements. The sink node in the network can either be mobile or static.

One of the main features of wireless sensor networks is self-organization mechanism [4] to configure the network by determining the neighboring nodes and routing table. In some applications where wireless sensor nodes are mobile, sensor nodes may stop working because its energy gets consumed faster or due to other failures. Scalability of sensor nodes is another feature. Sensor networks vary from several nodes to thousands. The deployment density is also different for different applications. For sensing and collecting data, the node density might reach the level where a node has several thousand other nodes in their transmission range. The protocols associated in sensor networks need to be accessible to these levels and should be able to maintain acceptable performance. When a node cannot directly communicate with the gateway, they use multihop routing through other nodes for the transmission. Ad-hoc wireless networks and wireless sensor networks have some similarities in their infrastructure less nature and multihop routing etc. But the number of sensor nodes in a wireless sensor network can be several orders of magnitude than the nodes in a wireless ad hoc network. Wireless sensor nodes are densely deployed and they are liable to failure. Moreover, the topology may change very frequently .Sensor nodes mainly use broadcasting patterns whereas traditional networks are based on point-to-point communication [3], [5].Moreover, the factor that distinguishes wireless sensor networks from traditional mobile ad-hoc networks is that the aim is the detection/estimation of some events of interest, and not just communication. So, sensor nodes are inadequate with power, computational capabilities, and memory. So, they are prone to physical attacks as they are unprotected in unsupervised areas. Also the broadcast and fluctuating nature of wireless medium makes WSN more vulnerable to security threats.

Wireless sensor networks have many applications in scenarios such as military target tracking and surveillance [2], natural disaster relief, biomedical health monitoring, hazardous environment exploration, seismic sensing etc. With natural disasters, sensor nodes can sense and detect the environment to forecast disasters before they occur like forest fire, weather forecasting, earthquakes and eruptions. In health applications, surgical implants of sensors can help to monitor a patient's health. . In military target tracking and surveillance, a WSN can support in intrusion detection and identification.

These applications cannot promise for the security of nodes to some extent, since they are unattended in nature after they are deployed. Recent researches on wireless sensor network are to integrate security in the design of each and every component of WSN.

The goal of this paper is to taxonomies the general security attacks in wireless sensor networks. Section II gives an overview of security goals in wireless sensor networks. The

general classification of security attacks is described in section III. Section IV summarizes the attacks in routing layer and section V concludes the paper.

II. SECURITY GOALS IN WIRELESS SENSOR NETWORKS

In real world, if every individual node in a network receives all the messages intended to it even in the presence of an adversary, that network is said to be guaranteed by the security goals [6] such as data confidentiality, authenticity, integrity of data, availability and data freshness.

Data confidentiality: Data confidentiality is an important aspect in network security. It is the ability to secure the message from a passive attacker so that any message communicated via network remaining confidential. It ensures that the data will not be leaked by unauthorized parties.

Authenticity: Data authentication verifies the identity of the senders and receivers .It ensures that the message has come from the legitimate user. The wireless nature of the media and the nature of unattended nodes are challenges which requires the need of authentication. Message authentication code (MAC) is used on the communicated data to accomplish data authentication.

Integrity of data: Data integrity ensures that the message has not been tampered or modified by an unauthorised user in the network. The unstable conditions due to wireless channel may cause loss of data. Any malicious node in the network also causes data alteration.

Availability and Data freshness: It is important to ensure that the data provided by any network is fresh and available at all times. Data freshness ensures that a third party cannot replay old messages in future. Availability is of crucial significance in operational applications.

III. SECURITY ATTACKS IN WIRELESS SENSOR NETWORKS

The broadcast nature of the transmission medium in wireless sensor networks make them vulnerable to security attacks. Furthermore, since the nodes are deployed at random in hostile environment, the threats become more serious. Many classifications of security threats in sensor networks have been done. The more common classifications are given below.

A. Passive Attacks

In passive attacks [7] an unsecure traffic is continuously monitored to collect the sensitive information from the network so that this information can be used for launching some other severe attacks. Passive attacks mostly act against the data confidentiality of network. Hence, there occurs disclosure of data files and information of the users by an unauthorised party. The network information is neither modified nor changed. Examples for passive attacks are given below:

Monitor and eavesdropping: As the name indicates the communication between nodes in a network is monitored by an adversary node to get details regarding transmitter data. Since the wireless sensor network has wireless transmission medium which is common to all the users, the monitoring and eavesdropping is a common type of attack. By encrypting the data, data dropping can be avoided. But when attacks occur together with other types of attacks, encryption cannot provide sufficient security.

Traffic analysis: Traffic analysis is nothing but acquiring knowledge about the communication patterns in a network by the adversary user. Adversary can cause malicious harm to some portion of a network or the entire network even if encryption of data has been done. Thereby sufficient information is analysed by the attacker.

Camouflage Adversaries: In a wireless sensor network some adversaries can introduce their own nodes or make some nodes compromised. These compromised nodes also known as camouflage nodes. They can masquerade the other sensor nodes in the network and misbehave as normal nodes to make fault routing information and can analyse the private details in such a way that way forward packets from the normal nodes through them.

B. Active Attacks

In active attack [9], an unauthorized attacker monitors the network, listen the channel and can modify the data stream in the communication channel. Active attack includes denial of service attacks, node malfunction, node replication attacks, false node, and passive information gathering etc. Routing layer attacks are active attacks which are explained in next section.

C. Host based vs. Network based attacks

Host based attacks are further classified in to three. In User compromise attack, the users are falsely assigned to disclose sensitive information about the network. Example, passwords and keys of nodes. In hardware compromise, the operations tinkers the hardware in order to take out the program code, data and key stored from hardware. In the case of software operations it is a software compromised attack. The network based attack deviates the protocols from its pre-planned functioning. It does not provide services like data availability, confidentiality, integrity and authenticity of the network.

D. Layer oriented attacks

Wireless sensor network has a functional layered architecture. Layered architecture enhances the robustness of the network by circumscribing the interactions of layers. Each layer is vulnerable to different denial-of-service attacks and the interaction between multiple

layers affects the entire architecture of the network and its communication paradigm.

- **Physical layer**

At the physical layer the attacks aim towards physical destruction of nodes and at signal frequencies which is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption functions. Deployment of nodes in hostile environments where attacker can physically access is a threat in physical layer.

Jamming: Sensor nodes use Radio Frequency (RF) to communicate each other. In jamming attacks, the malicious nodes are introduced by the adversary in order to continuously send high energy signals to make the networks busy. So the important communication will be interrupted. Spread spectrum communication [9] like frequency hopping can be provided to protect from jamming attacks.

Tampering: An attacker can damage or replace sensor and computation hardware and the program codes or remove sensitive materials like cryptographic keys to allow unrestricted access to higher levels of communication. Thereby these tampering nodes interfere in the physical access of sensor nodes.

- **Data Link layer**

The data link layer provides the point-to-point communication access to sensor nodes in the wireless media by Media Control Access (MAC), for example CSMA. Link layer also provides error detection, error correction and data encoding .The main attacks in Link layer are

Collision: Basically the collision [10] occurs when two or more nodes try to access the common channel for the transmission in the same frequency simultaneously. So, the adversary will make the chances for make collisions in the channel. This may alter the message content; or even discard the packets at the destination.

Exhaustion: Exhaustion also called continuous channel access in which attacker interrupts the channel access by continuously sending data transmission requests over the channel. So, other nodes get starved for the channel. By using efficient Time Division Multiplexing (TDMA), it can be avoided to some extent.

- **Network layer**

The goal of network routing layer is to provide reliable end-to-end transmission. The routing protocols have to be energy and memory efficient but along with that they have to be healthy to security attacks and node failures. There have been many power-efficient routing protocols proposed for sensor networks. Wireless sensor network attacks target the network layer in order to change the path information from sensor nodes to the sink node. They take advantage of the routing protocol that is used by the network in order to attract all the transmission from other nodes through the adversaries. Since Routing layer is responsible for routing of messages from nodes to nodes and nodes to sink node, any delay or drop in the packets may cause loss in data information. Many denial of service attacks occur in network layer which are described in next section in detail.

IV. NETWORK LAYER ATTACKS

In network layer [11] the malicious nodes forward the data packets through them or delay them or drop the data either completely or based on any criteria. Many forms of DoS attacks are listed below.

Sinkhole attack: Sinkhole [12] attracts all the nodes through malicious advertising that it is the sink node so that the member nodes forward the data towards them unknowingly. Sinkhole attack can either interfere with routing packets, spoof or replay route messages, or even transmit false report attacks, making the compromise node a more attractive path to forward their packets.

Selective forwarding attack: In selective forwarding attack [13] only certain packets are selectively dropped by the malicious node. This results in an unfaithful transmission of data. The selectively drop the packets either by the node ID or based on time interval or packet content, size, the source node etc. or delay the transmission. The relevant information is lost in the communication network. In the cases where all the packets are dropped and nothing is forwarded then it is called black hole attack. Multipath routing combined with Random selection of path to destination can be used for reduce the effect of selective forwarding attack. It is either termed as neglect and greed attack.

Wormhole attack: In wormhole attack [14] the adversary can tunnel the messages received in one part of the network to the other end through a low latency path consist of malicious nodes. Thereby misdirect the forwarding of relevant information. The distant nodes are made to appear so close to the sink node thereby exhaust the energy quickly.

Sybil attack: In Sybil attack [15] the adversary node fools the neighbor notes by having multiple identities and access information of other nodes. As the adversary occurs in multiple locations the Geographic routing protocols are mostly confused. Use of symmetric key may overcome this attack.

Hello flood attack: Hello flood attack [8],[10] uses hello packets which are commonly used in advertising communications in order to make traffic overhead. When a node receives such packet it unknowingly replies to it by sending packets. Hello flood attack is an injurious active attack. It causes bandwidth wastage.

Spoofed, altered, replayed packets: This attack targets the routing information used by nodes. As a result, it could lead to creating routing loops, or increase the end to end delay. The attacker can delay, spoof [16], alter or replay the packets in order to create an overhead in the network.

V. CONCLUSION

Wireless Sensor networks have become an auspicious future for many applications. In the absence of an adequate security, deployment of sensor networks is vulnerable to a variety of attacks. Sensor node's limitations and nature of wireless communication poses unique security challenges. The goal of this paper is to give a comprehensive taxonomy of the security attacks on sensor networks and their effect on the performance of the network. Moreover, future directions for an extended research in the area of sensor network security are also provided.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci "Wireless sensor networks: a survey", Computer Networks 38 (2002), Elsevier

[2] G. Simon, M. Maroti, A. Ledeczi, G. Balogh, B. Kusy, A. Nadas, G. Pap, J. Sallai, K. Frampton, "Sensor network-based countersniper system, in: Proceedings of the Second International Conference on Embedded Networked Sensor Systems (Sensys), 2004.

[3] C. Perkins, "Ad Hoc Networks", Addison-Wesley, Reading, MA, 2000

[4] S. Toumpis, T. Tassiulas, Optimal deployment of large wireless sensor networks, IEEE Transactions on Information Theory 52 (2006) 2935–2953.

[5] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and Countermeasures, Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, Vol. 1, No. 2-3, pp. 293-315, 2003.

[6] Dr. G. Padmavathi, Mrs. D. Shanmugapriya,"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks",IJCSIS) International Journal of Computer Science and Information Security, 2009

[7] Tanya Roosta, Shiuhpyng Shieh ,Shankar Sastry, "Taxonomy of Security Attacks in Sensor Networks and Countermeasures",First IEEE International conference on System integration and Reliability improvements,2006.

[8] Pooja, Dr R K Chauhan, "Review on security attacks and countermeasures in wireless sensor networks",International Journal of advanced research in computer science 2017.

[9] Xu, W., Trappe, W., Zhang, Y., and Wood, T, The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. ACM MobiHoc'05, May 25–27, 2005, Urbana-Champaign, Illinois, USA, pp 46-57

[10] David R. Raymond and Scott F. Midkiff,(2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81

[11] Christiana Ioannou and Vasos Vassiliou , "The Impact of Network Layer Attacks in Wireless Sensor Networks" 2016 International Workshop on Secure Internet of Things.

[12] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks," in Algorithmic Aspects of Wireless Sensor Networks (M. Kutyowski, J. Cicho, and P. Kubiak, eds.), vol. 4837 of Lecture Notes in Computer Science, pp. 150–161, Springer Berlin Heidelberg, 2008.

[13] Devu Manikantan Shila, Yu Cheng, and Tricha Anjali, "Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs", Ieee Transactions On Wireless Communications, Vol. 9, No. 5, May 2010.

[14] Y.C. Hu, A. Perrig, and D. Johnson, "Leashes: a Defense Against Wormhole Attacks in Wireless Networks," in INFOCOM 2003. Twenty- Second Annual Joint Conference of the IEEE Computer and Communications, 2003.

[15] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," in Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, IPSN 2004.

[16] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized Protocol Stack for the Internet of (Important) Things," IEEE Communications Surveys Tutorials, 2013.

[17] A. D. Wood and J. A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks," Handbook of Sensor Networks:Compact Wireless and Wired Sensing Systems, pp. 739–763, 2004.

[18] Guangjie Han, Wen Shen, Trung Q. Duong, Mohsen Guizani and Takahiro Hara ," A proposed security scheme against Denial of Service attacks in cluster-based wireless sensor networks, security and communication networks Security Comm. Networks (2011).