ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Survey on Security Attacks in Wireless Sensor Networks

Satveer Kaur
Assistant Professor
Dashmes Khalsa College
Zirakpur

Nitika Goyal
Assistant Professor
Guru Nanak College
Budhlada

Abstract-Wireless sensor networks have become an emergent area of research and development due to the marvelous number of applications such as battlefield, building, traffic surveillance, habitat monitoring and smart homes and many more. These applications can greatly benefit from such systems. The area has lead to the development of tiny, cheap, disposable and self contained battery powered computers. These computers are known as sensor nodes or "motes". These can accept input from an attached sensor, process input data and transmit the results wirelessly to the transit network. These networks are easily prone to security attacks due to the wireless nature as after deployment; these networks are unattended and nodes are often placed in a hostile or dangerous environment where they are physically unprotected. The inherent power and memory limitations of sensor nodes make conventional security solutions unfeasible. There are a lot of attacks which affect the WSN's security. Some of these attacks are selective forwarding, sinkhole, denial of service etc. In this paper, we discussed about all these security attacks faced by WSNs.

Keywords: WSN, Security, Attacks, DoS, MAC.

I. INTRODUCTION

Wireless sensor networks are mostly designed for real-time collection and analysis of low level data in hostile environments. They are well suited to a significant amount of monitoring and surveillance applications. The popular applications of WSN include battlefield, building, traffic surveillance, habitat monitoring and smart homes, wildlife monitoring, bushfire response, distributed robotics etc. Majority of the sensor networks are deployed in hostile and dangerous environments. Hence security is an important issue. Providing security in WSNs is even very difficult due to the resource limitations of sensor nodes. However in the next section, the security attacks are discussed.

II. Security attacks in Wireless sensor networks

Wireless sensor networks are power constraint networks. They have limited computational and energy resources. This makes them vulnerable to be attacked by any attacker who is deploying more resources than any individual node or any base station. It may not be difficult job for the attacker. Also these networks are vulnerable to security attacks due to the broadcast nature of the transmission medium and the hostile and dangerous networks where the nodes are placed. Therefore the nodes are not physically safe. Here are some principal types of attacks which are concerned to WSNs.

i.) **Node Capture Attack:** In this attack, an attacker captures the sensor nodes physically and gains full control over the nodes. He compromises the nodes so that sensor readings sensed by compromised nodes are inaccurate or manipulated. The attacker can easily extract cryptographic keys and obtain unlimited access to the information stored on the memory chip of the captured node with the potential to damage the entire WSN [1][2].

ii.) **Denial of Service (DoS):** It is an attempt to make a network unavailable for its legitimate users. An attacker tampers with data before it is used by sensor nodes, resulting in false readings and therefore leads to wrong decisions. When an attacker continuously attacks a targeted access point or network with spurious requests, premature successful connection messages, failure messages, Denial-of-service attack occurs. DoS is an event that eliminates or reduces a network's capacity to perform its expected functions through resource exhaustion, malicious broadcasting of high energy signals, hardware failures or software bugs [1][2].

iii.) **Software Attacks:** In this attack, the attacker may try to break the running software on the sensor node or modify the software code in memory or exploit known weaknesses in the software code. Chances are the operating system or the applications running in a sensor node are vulnerable to popular exploits. A well known example of such an attack is buffer overflow attack where a process attempts to store data outside the boundaries of a fixed length buffer, resulting in the extra data overwriting the adjacent memory locations [2][3].

iv.) **Traffic Analysis:** In WSNs, all communication moves toward a base station in many-to-one or many-to-few patterns. An attacker attempts to gain knowledge of the network, traffic, and behavior of nodes. Even when the messages transferred are encrypted, it still leaves a high possibility of analysis of the communication patterns. It may include examining the message length, message pattern or coding, and duration the message stayed in the router. In addition to this, the attacker can associate all incoming and outgoing packets at any router or member. This type of attack violates privacy and can harm members or routers for being linked with messages [1][2][4].

v.) **Sybil Attack:** This type of attack is much prominent in Link layer. In this attack, a single node duplicates itself and presents itself to other nodes with multiple spoofed identifications. The Sybil attack targets fault tolerant schemes such as distributed storage, multiple routing and topology maintenance [3][4].

vi.) **Wormhole Attack:** In this attack, attackers are strategically placed at different ends of a network. Attacker receives packets (or bits) at one point of network, “tunnels” them to another point of network and then retransmits them into the network from that point. This is usually done with the coordination of two opponent nodes. The nodes try to understate their distance from each other by broadcasting packets along an out-of-bound channel that is available to the attacker. An attacker intrudes communication initiated by sender, by copying a portion or a whole packet, and speeds up sending the copied packet through a specific wormhole tunnel in such a way that the copied packet arrives before the original packet at the destination [1][3][4].

vii.) **Impersonate Attack:** An attacker, in this attack, impersonates another node’s identity, either MAC or IP address, to establish a connection with or launch other attacks on a victim. The attacker may also use the victim’s identity to establish a connection with other nodes or launch other attacks on behalf of the victim [1][5].

viii.) **Sinkhole Attack:** Also known as black holes occur at the network layer. The adversary’s aim is to tempt nearly all the traffic from a particular area through a compromised node, in the sense that it promotes zero-cost routes to neighboring nodes with respect to the routing algorithm. This results maximum traffic to flow towards these fake nodes [6][7][8].

ix.) **Selective Forwarding Attack:** A node plays the role of router. In this type of attack, the adversary includes itself in a data flow path of interest. It is the situation where certain nodes do not forward many of the messages they receive and simply drop them. The sensor networks depend on repeated forwarding by broadcast for messages to propagate throughout the network [4][5][9].

x.) **Hello Flood Attacks:** This attack exploits HELLO packets that are needed in many protocols to announce nodes to their neighbors. A node receiving this message may consider that it is within radio locality of the sensor. An attacker with a high radio transmission range and processing power sends HELLO packet to a number of sensor nodes within a WSN. It gives an illusion that the malicious node is their neighbor. This causes a large number of nodes sending packets to this imaginary and thus into oblivion [3][6][8].

xi.) **Flooding:** It also occurs at network layer. An attacker using this type of attack, normally sends a large number of packets to the victim or to an access point to prevent the victim or the entire network from establishing or continuing communications. To hit each request, some resources are allotted to the adversary by the targeted node. It may result into effusion of the memory and energy resources of the attacked node [1][6].

xii.) **De-synchronization:** It occurs at the transport layer. This attack tries to disturb an existing connection. Attacker copies messages between endpoints. Modifications in sequence numbers and control flags are usually made. It might prevent the endpoints from exchanging messages by continuously requesting retransmission of lost message. It leads to an infinite retransmission cycle that exhausts a lot of energy [1][6].

xiii.) **Jamming:** It is the well known attack at physical layer of WSN. It consists of intentionally disturbing the radio channel by sending useless information on the frequency band to disrupt the signal transmission. Jamming can be of two types- constant and intermittent. Constant jamming affects the complete obstruct of the whole network whereas in intermittent jamming, nodes are capable of communicating periodically but not continuously [5][6][9].

xiv.) **Node Replication Attack:** This attack is quite simple. It is based upon giving the same identity to different physical nodes. Every sensor node in the network has a unique ID. An attacker seeks to add a node to an existing sensor network by copying the nodeID of an existing sensor node. By using the replicated node, packets can be corrupted or even misrouted or modified. Malicious node can get authority to access sensitive information and can harm the whole network [4][6].

xv.) **Physical Attacks:** Sensor networks are usually operated in hostile and dangerous outdoor environments. The sensor deployment is unattended. Physical attacks destroy sensor nodes permanently. The loss is irreversible. An attacker can extract sensitive information. Tampering with the associated circuitry and cryptographic secrets are results of physical access to the node by an attacker [3][4].

xvi.) **False or Malicious Node:** Most of the attacks in WSNs are due to the insertion of the false information by the compromised nodes within the network. A false or malicious node involves the addition of a node by an attacker and causes the injection of malicious data. An intruder might add a node to system that provides false data or prevents the passage of true data. Malicious code injected in the network could spread to all nodes, potentially whole network [4][7].

xvii.) **Spoofed, Altered, or Replayed Routing Information:** The most direct attack against routing is to target the routing information while being exchanged between nodes. An attacker may be able to create routing loops, attract network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end delay [3][8].

xviii.) **Collision Attack:** Collision is a type of link layer jamming that occurs when two or more nodes attempt to transmit data at the same time and at the same frequency. When packets collide, a change will likely to occur in the data portion, causing a checksum mismatch at the receiving end. The packet will be discarded as invalid. An attacker may cause collisions in particular packets such as ACK control messages. This type of attack reduces the network performance [3][6].

xix.) **Monitor and Eavesdropping:** Eavesdropping is the process of detecting the contents of communication by overhearing attempt to data and gathering information from a network. The information remains the same but the privacy is compromised. The effects of this attack are extracting sensitive and confidential information [1][10].

xx.) **Node Outage:** It is the situation that occurs when a node stops its function and the attacks apply physically or logically in network. The effects of this attack are stopping the node services such as reading, gathering and launching the functions [4][10].

xxi.) **Exhaustion:** It occurs at data link layer. The attacker dominates the power resources of the nodes by causing them to retransmit the message even when there is no collision or obliging it to do calculations or to receive or transmit unnecessarily [5][6][10].

III. Conclusion

Wireless Sensor Networks provide a various type of opportunities for increasing productivity in various fields and minimizing costs. But as WSNs are usually deployed in hostile and dangerous environments, a lot of security threats and attacks are vulnerable which can put the networks in critical situations. A number of security attacks are discussed in this paper. Still a lot of attacks remain to identify.

IV. References

[1] K.Venkatraman, J.VijayDaniel, G.Murugaboopathi," Various Attacks in Wireless Sensor Network: Survey", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol. 3, Issue 1, March 2013.

[2] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim," A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks", Journal of Security Engineering, Vol. 9, Issue 3,2012.

[3] Kavitha Tamil, D. Sridharan, "Security Vulnerabilities In Wireless Sensor Networks: A Survey", Journal of Information Assurance and Security, Vol. 5, 031-044, 2010.

[4] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, pp. 1 & 2, 2009.

[5] Mohamed-Lamine Messai, "Classification of Attacks in Wireless Sensor Networks", International Congress on Telecommunication and Application'14,University of A.MIRA Bejaia, Algeria, 23rd-24th April 2014.

[6] Aashima Singla, Ratika Sachdeva, " Review on Security Issues and Attacks in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 4, April 2013

[7] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[8] Sushma, Deepak Nandal, Vikas Nandal, "Security Threats in Wireless Sensor Networks", International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011.

[9] Mr. Manish M Patel, Dr. Akshai Aggarwal, "Security Attacks in Wireless Sensor Networks: A Survey", International Conference on Intelligent Systems and Signal Processing, March 2013.

[10] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi, "Security Issues and Attacks in Wireless Sensor Network", World Applied Science, Journal 30 (10): 1224-1227, 2014.