Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Wireless Sensor Network Security: Vulnerabilities, Threats and Countermeasures

R. Rathika, D. Sowmyadevi
Assistant Professor, Department of Computer Science,
Sri Ramakrishna College of Arts and Science for Women, Coimbatore,
Tamilnadu, India

Abstract*— Wireless Internet access technology is being increasingly deployed in all areas like MNC and public environments, as well as by the Internet users at home. It becomes extremely important to all internet users. A Wireless Network is a wireless communication system that allows computers and workstations to communicate and exchange data with each other using electromagnetic waves as the transmission medium. Wireless sensor network is a combination of tiny devices called as sensor nodes which have computing, sensing and processing capabilities. Security is a major important issue in wireless network. End users are not security experts, and may not be aware of the risks posed by wireless networks. Effective management of the threats associated with wireless technology requires a sound and systematic evaluation of risk given the environment and development of a plan to mitigate identified threats. This paper deals with the security aspects in each layer in the wireless sensor networks giving the probable counter measure for the same.

***Keywords*— Wireless Sensor Network, Security, Sensor nodes, Threats, Attacks on Layers**

I. INTRODUCTION

Wireless networking presents many advantages Productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. The concerns for wireless security, in terms of threats, and countermeasures, are similar to those found in a wired environment, such as an Ethernet LAN or a wired wide-area network. The security requirements are the same in both environments: confidentiality, integrity, availability, authenticity, and accountability. However, some of the security threats are exacerbated in a wireless environment and some are unique to the wireless environment. The most significant source of risk in wireless networks is the underlying communications medium. In addition, there have traditionally been security risks in wireless protocols that have only been addressed in relatively recent generations of these protocols. WLAN is commonly referred to as "Wi-Fi" (wireless fidelity). Wireless local area networks give freedom to one move their wireless devices from one place to other within their offices and organizations without the need for wires and without losing network connectivity. Nowadays wireless networks are used in many areas such as in universities, healthcare-centres, hospitals, police departments, military and airports. Therefore, it is very important to enhance the wireless network security in order to protect the information of the network. Different network security protocols have been developed to secure the wireless network, among which are WEP, WPA, and WPA2. Because radio waves can pass through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors or even outside the building, it gives opportunity to attackers to intercept the information that can be used to launch different types of attacks. Therefore, it is important to know different kind of security attacks at different layers in order to defend the wireless networks.

II. OPERATION IN WSN

In computer networking there is a great value of wireless networking because it has no difficult installation, no more expenditure and has lot of way to save money and time. In the field of wireless networking there is another form of networking which is called as wireless sensor network. A type of wireless networking which is comprised on number of numerous sensors and they are interlinked or connected with each other for performing the same function collectively or cooperatively for the sake of checking and balancing the environmental factors. This type of networking is called as Wireless sensor networking. Basically wireless sensor networking is used for monitoring the physical conditions such as weather conditions, regularity of temperature, different kinds of vibrations and also deals in the field of technology related to sound.

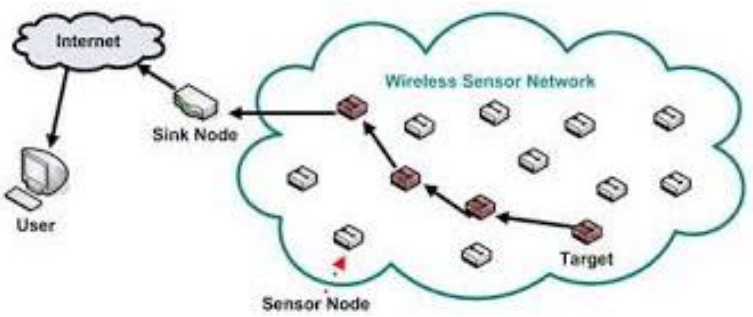

Fig. 1 Architecure of Wireless Sensor Nodes

Total working of wireless sensor networking is based on its construction. Sensor network initially consists of small or large nodes called as sensor nodes. A sensor node, also known as a mote.

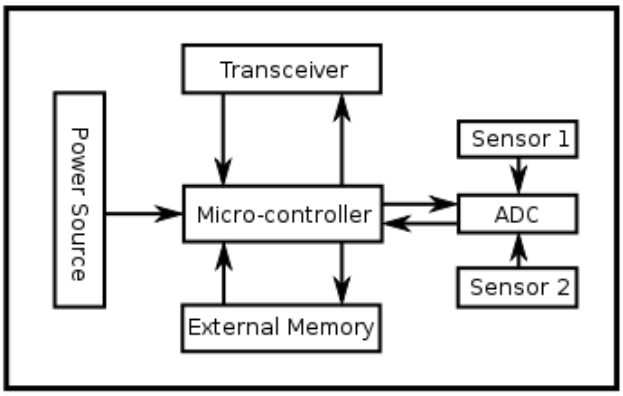

Fig. 2 Structure of Node

These nodes are varying in size and totally depend on the size because different sizes of sensor nodes work efficiently in different fields. Wireless sensor networking have such sensor nodes which are specially designed in such a typical way that they have a microcontroller which controls the monitoring, a radio transceiver for generating radio waves, different type of wireless communicating devices and also equipped with an energy source such as battery. The entire network worked simultaneously by using different dimensions of sensors and worked on the phenomenon of multi routing algorithm which is also termed as wireless ad hoc networking.

III. DIFFERENT LAYER THREATS

Threats are entities that can attack networks through system vulnerabilities. Examples of threat are hackers, viruses and spywares that can cause disturbance in the network. Vulnerability is a weakness or flaw in operating system or software that can be exploited by a threat. Some examples are wireless networks not using encryption, weak passwords and Access Point sending wireless signals outside the building.

A. Sensor Network Security in Physical Layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption [1]. The most common attacks on physical layer are as follows:

Jamming

Jamming represents the most serious security threat in the field of Wireless Sensor Networks (WSNs), as it can easily put out of order even WSNs that utilize strong high layer security mechanisms. Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission [5]. An attacker can easily flood the 2.4 GHz frequency, corrupting the signal until the wireless network stops to function. Other devices that operate on the 2.4 GHz band such as Bluetooth Devices, Car Alarms and oven can also disrupt a wireless network using this frequency. Jamming is also widely used to launch Denial of Service (DoS) attacks at the physical layer. A DoS attack is an attacker's attempt to exhaust the resources available to its users. Jamming can be avoided by using spreading techniques. A wireless intrusion detection/prevention system (IDS/IPS) can also be used to defend the wireless network against jamming. There are four types of jamming attack such as constant jammer, deceptive jammer, random jammer, reactive jammer.

Tampering

Tampering Sometimes the nodes are physically tampered by an adversary. Such condition is called tampering [3]. A tampering attacker may damage, replace and electronically interrogate the nodes to get information [4]. One defence to this attack involves tamper-proofing the node's physical package. Self Destruction (tamper-proofing packages)-whenever somebody accesses the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information. Second-Fault Tolerant Protocols-the protocols designed for a WSN should be flexible to this type of attacks.

B. Sensor Network Security in Data Link Layer

The goal of this Layer is to insure interoperability amongst communication between nodes to nodes. The Data Link layer is responsible for the multiplexing of data streams, data frame detection, medium access, and error control [1]. The data link layer is vulnerable due to the reason that the data is transmitted in an open insecure medium. Hence it is vulnerable to the attacks on the authenticity, integrity and confidentiality of the data being routed[5]. The main attacks at the data link layer are as follows:

Collision

A collision occurs when two nodes attempt to transmit on the same frequency concurrently. When packets collide, a change will occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid .A typical defence against collisions is to use error- correcting codes.

Continuous Channel Access (Exhaustion)

A malicious node disrupts the Media Access Control protocol, by continuously requesting or transmitting over the channel. This leads a starvation for other nodes in the network with respect to channel access. One of the countermeasures to such an attack is Rate Limiting to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions. A second technique is to use time division multiplexing where each node is allotted a time slot in which it can transmit.

C. Sensor network security issues at Network layer

The goal of Network layer is to find the best path for well-organized routing mechanism. This layer is responsible for routing the data from node to node, node to sink ,node to base station, node to cluster head and vice versa. Vulnerabilities at network layer are as follows:

Selective Forwarding

Normally the sensor networks are multi-hop systems. So, the sensors pass information from one end to the base station by routing them through intermediate nodes. Malicious node may be present within the network path. In a flooding based protocol, the attacker (malicious node) listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. [7] Then the target may choose the route which contains the malicious node. Malicious or attacking nodes can however refuse to route certain messages and drop them. The result is loss of huge amount of data, during the multi-hop information exchange process. In another case it may happen that the malicious node drops all the packets it receives, hence no information is forwarded. This creates a black hole. Such attacks are effective when the attacker is openly included in the data path of sensor network. One defence against selective forwarding attacks is using multiple paths to send data [6].A second defence is to detect the malicious node or assume it has failed and seek an alternative route.

Denial of service

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

Sinkhole Attack

Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes. [8]. Since now most of the data is being routed through the malicious node, the attacker/malicious node can play anything with the sensor data. [9] Many other attacks such as wormhole, selective forwarding or eavesdropping can be initiated through this sinkhole attack. Geo-routing protocols are known as one of the routing protocol classes that are resistant to sinkhole attacks, because that topology is constructed using only localized information, and the traffic is naturally routed through the physical location of the sink node, which makes it difficult to lure it elsewhere to create a sinkhole.

Sybil Attack

A faulty node or an adversary may present multiple identities to a peer-to-peer network in order to appear and function as multiple distinct nodes. After becoming part of the peer-to-peer network, the adversary may then overhear communications or act maliciously. By masquerading and presenting multiple identities, the adversary can control the network substantially. Communication to an illegal node results in data loss and becomes dangerous in the network.

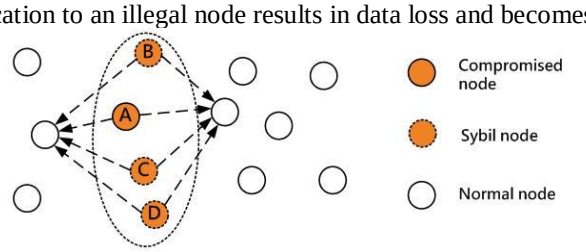

Fig. 3 Sybil Attack

Wormholes Attacks

Two powerful adversary nodes placed in two strategic locations. Advertise a low cost path to the sink. All nodes in the network are attracted to them looking for an optimal route. This is attack is usually applied in conjunction with

selective forwarding or eavesdropping attack. Two powerful adversary nodes placed in two strategic locations. Advertise a low cost path to the sink. All nodes in the network are attracted to them looking for an optimal route. This is attack is usually applied in conjunction with selective forwarding or eavesdropping attack.

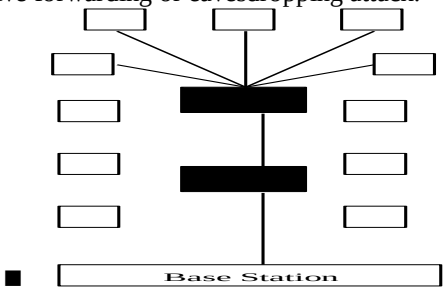

Fig. 4 Wormhole Attack

Hello Flood Attacks

Many protocols which use HELLO packets make the naive assumption that receiving such a packet means the sender is within radio range and is therefore a neighbour. An attacker may use a high-powered transmitter to trick a large area of nodes into believing they are neighbours of that transmitting node [7]. If the attacker falsely broad casts a superior route to the base station, all of these nodes will attempt transmission to the attacking node, despite many being out of radio range in reality.

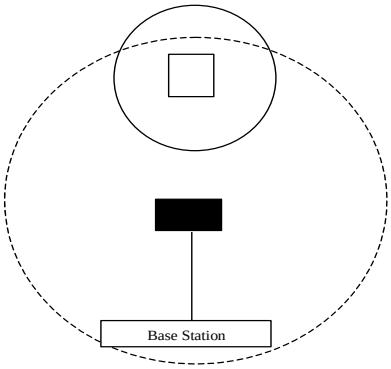

Fig. 5 Hello Flood Attacks

Acknowledgment Spoofing

Routing algorithms used in sensor networks sometimes require Acknowledgments to be used. An attacking node can spoof the Acknowledgments of overheard packets destined for neighbouring nodes in order to provide false information to those neighbouring nodes . An example of such false information is claiming that a node is alive when in fact it is dead.

D. Sensor network security issues at Transport layer

The transport layer is responsible for managing end-to-end connections [1].Sometimes an attacker might be strong enough to reach up to the transport layer, due to attack being undetected at the lower layers[3]. Two possible attacks in this layer, flooding and de-synchronization.

Flooding

An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes. One proposed solution to this problem is to require that each connecting client demonstrate its commitment to the connection by solving a puzzle. As a defence against this type of attack, a limit can be put on the number of connections from a particular node.

De-synchronization Attacks

In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence these messages are again transmitted and if the adversary maintains a proper timing it can prevent the endpoints from exchanging any useful information .This will cause a great drainage of energy of legitimate nodes in the network in an continual synchronization-recovery protocol. A possible solution to this type of attack is to require authentication of all the packets including control fields communication between hosts. Header or full packet authentication can overcome such an attack.

E. Sensor network security issues at Application layer

The goal of Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results. Main attack at application layer is attacks on reliability.

Attacks on reliability

If an adversary changes the data in one path then it puts a question mark on the reliability of the data. In this attack attacker needs to identify the path of communication and put adversary in that path to change the data. An adversary can

produce false data or query by joining the network. When a node responds to these wrong data or query, leads them to suffer from the energy drain attack. Usually to ensure reliability acknowledgement is expected for each successful data delivery.

IV. SECURING WIRELESS TRANSMISSIONS

The nature of wireless communications creates three basic threats: Interception, Alteration and Disruption.

Protecting the Confidentiality of Wireless Transmissions

Two types of countermeasures exist for reducing the risk of eavesdropping on wireless transmissions. The first involves methods for making it more difficult to locate and intercept the wireless signals. The second involves the use of encryption to preserve confidentiality even if the wireless signal is intercepted.

Preventing Alteration of Intercepted Communications

Interception and alteration of wireless transmissions represents a form of "man-in the middle" attack. Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users.

Countermeasures to Reduce the Risk of Denial-of-Service Attacks

Wireless communications are also vulnerable to denial-of-service (DoS) attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Careful site surveys can identify locations where signals from other devices exist; the results of such surveys should be used when deciding where to locate wireless access points. Regular periodic audits of wireless networking activity and performance can identify problem areas; appropriate remedial actions may include removal of the offending devices or measures to increase signal strength and coverage within the problem area.

V. CONCLUSION

Wireless sensor network is a growing field and has many different applications. Most security threats to wireless ad-hoc network are applicable to wireless sensor network. These threats are further complicated by the physical limitations of sensor nodes. Some of these threats can be countered by encryption, data integrity and authentication. Security of wireless sensor network remains an intensive studied field. But wireless sensor networking has a bright future in the field of computer networking because we can solve the monitoring problems at an advanced level in the future with the help of such technology of networking.

REFERENCES

[1] I.F.Akyildiz et al.,"A Survey on Sensor Networks",IEEE Commun.Mag.,vol.40,no.8,Aug.2002,pp.102-114.

[2] Laiali Almazaydeh Et Al "Performance Evaluation Of Routing protocols In Wireless Sensor Networks" International Journal Of Computer Science And Information Technology, Volume 2, Number 2, April 2010

[3] Madhumita panda " Security Threats at Each Layer of Wireless Sensor Networks" ijarcsse Volume 3, Issue 11, November 2013

[4] Rajinder singh " wireless network security main threats at different layers" international journal of wired and wireless communications vol.1, issue 1, october, 2012

[5] M. Yasir Malik" An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations" Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management DOI: 10.4018/978-1-4666-0101-7.ch024

[6] C.Karlof and D.Wagner,"Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" ,Proc. First IEEE Int'l Wksp. Sensor Network Protocols and Applications ,May 2003,pp.113-27.

[7] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong,"Security in Wireless Sensor Networks: Issues and Challenges", International Conference on Advaificances in Space Technologies.

[8] Aristides Mpitziopoulos Et Al "A Survey On Jamming Attacks And Countermeasures In Wsns" IEEE Communications Surveys & Tutorials, Vol. 11, No. 4, Fourth Quarter 2009

[9] Qusay Idrees Sarhan " Security Attacks And Countermeasures For Wireless Sensor Networks: Survey" International Journal Of Current Engineering And Technology Issn 2277 - 4106 © 2013 Inpressco.

[10] Min-kyu Choi et al " Wireless Network Security:Vulnerabilities, Threats and Countermeasures" International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008

[11] Dr. G. Padmavathi et al "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009

[12] *Bhavik Doshi "* Wireless Network Security*" Privacy and Security Winter 2008-09*

