ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVAY ON SECURITY ISSUES AND ATTACKS IN WIRELESS SENSOR NETWORK

Minakshi Sharma*, Sakshi Kalra, Chanda Monga

* PG Department of Computer Science, Dev Samaj College for Women Ferozepur City,Ferozepur, Punjab, India

DOI: 10.5281/zenodo.48314

ABSTRACT

Wireless sensor network is the most growing technology for sensing and performing the different tasks. With the beginning of the internet, security has become a major concern and the history of security allows a better understanding of the emergence of security technology. The intent of this paper is to consider the protection correlated issues and incitements in wireless sensor networks. We identify the security threats, appraisal anticipated security mechanisms for wireless sensor networks. The inclusion of wireless communication technology also incurs various types of security threats due to non consideration installation of sensor nodes as sensor networks may interact with sensitive data and operate in hostile unattended environments.

KEYWORDS: Wireless Sensor Technology, Security , Attacks, Wireless Local Area Network (WLAN).

INTRODUCTION

A wireless sensor network is a group of particular transducers with a communications transportation for monitoring and demo conditions at dissimilar locations. Commonly monitored parameters are temperature, humidity, anxiety, wind direction and velocity, lighting , vibration intensity, sound intensity, power-line voltage, chemical concentrations, impurity levels and vital body functions. The basic idea of sensor network is to disperse miniature sensing devices; which are capable of sensing some changes of parameters and communicating with other devices, over a specific geographic area for some particular purposes like goal tracking, supervision, conservation monitoring etc. The eye-catching features of the Wireless Sensor Networks concerned many researchers to work on various issues related to these types of networks. However, while the course-plotting strategies and wireless sensor network modeling are getting much preference, the defense issues are yet to entertain wide-ranging focus.

SECURITY

Wireless security is the avoidance of unauthorized access to computers using wireless networks. The most common types of wireless security are WEP and Wi-Fi Protected Access. WEP is a notoriously weak security standard. The password it uses can habitually be broken in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard, which was outdated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick substitute to develop security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware promote or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key the longer key span improve security over WEP.

Many laptop computers have wireless cards pre-installed. However, wireless networking is prone to some security issues. Hackers have originate wireless networks relatively easy to break and use wireless technology to hack into wired networks. So it is very important that enterprises define effective wireless security policies. WIPS or WIDS are frequently used to put into effect wireless security policies. Risks to users of wireless technology have augmented as the service has become more popular. There were few dangers when wireless technology was first introduced. Hackers had not yet had time to latch on latest technology, and wireless networks were not frequently found in the work place. However, there are many security risks allied with the current encryption methods, and in the carelessness and unawareness that exists at the user and commercial IT level. Hacking methods have become

much more sophisticated and innovative with wireless access. Hacking has also become much relaxing and available with easy-to-use Windows- or Linux-based tools.

Attacks: Attack aligned with Wireless Sensor Networks might be largely measured from two different levels of views. One is the attack in opposition to the safety mechanisms and another is against the essential mechanisms. Here we point out the foremost attacks in wireless sensor networks.

Denial of Service: Denial of Service is produced by the involuntary failure of nodes or malevolent action. The simplest DoS attack tries to fatigue the resources obtainable to the fatality node, by sending extra unnecessary packets and thus prevents justifiable system users from accessing possessions to which they are allowed. DoS attack is meant not only for the adversary's effort to subvert, interrupt, or demolish a network, but also for any event that diminishes a network's capability to provide a service.

Fig:1.1 Denial of Service

In Wireless Sensor Networks, numerous types of DoS attacks in dissimilar layers might be performed. At physical layer the DoS attacks could be congestion and tampering, at link layer, collision , fatigue , unfairness, at network layer, ignore and voracity , homing , Misdirection, black holes and at transfer layer this assault could be performed by spiteful flooding and desynchronization. The mechanisms to avoid DoS attacks include payment for network resources, repel, strong confirmation and detection of traffic.

Attacks on Information in transit: In a Sensor Network, Sensors supervise the change of specific parameters or standards and report to the sink according to the condition. While transferring the report, the information in transfer may be distorted, spoofed, replayed again or vanished. As wireless communication is exposed to eavesdropping, any invader can supervise the traffic flow and get into action to interrupt, seize, modify or construct [22] packets thus, provide wrong information to the base stations. As sensor nodes normally have short range of transmission and scarce resource, an invader with high processing power and larger communication range could assault several sensors at the same time to alter the real information during transmission.

Sybil Attack: The sensors in a Wireless Sensor Network force need to work together to achieve a task, hence they can use allotment of subtasks and idleness of information. In such circumstances, a node can imagine to be more than one node using the identities of other valid nodes. This type of attack where a node forges the identities of more than one node is the Sybil assault. Sybil assault tries to degrade the integrity of data, security and source consumption that the circulated algorithm attempts to accomplish. Sybil assault can be performed for attacking the spotted storage, routing mechanism, data aggregation, selection, fair resource allotment and misconduct exposure.

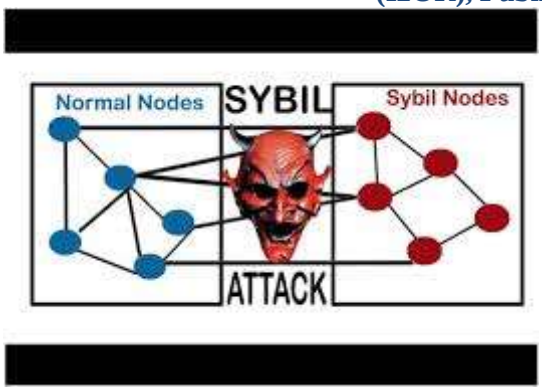

Fig 1.2 Sybil Attack

Basically, any peer-to-peer network is susceptible to Sybil assault. However, as WSNs can have some sort of base stations or gateways, this assault could be prevented using efficient protocols.

Sink Hole Attack: In sink hole attack, a malevolent knob acts as a sinkhole to magnetize all the traffic in the sensor network. Especially in a flooding based practice, the attacker listens to requests for routes then replies to the target nodes that it contains the direct path to the base station. Once the malicious device has been able to put in itself among the communicating nodes it is capable to do anything with the packets fleeting between them. In fact, this attack can affect even the nodes those are noticeably far from the base stations.

Hello Flood Attack: Hello Flood Attack is an significant attack on the network layer, in which an opposition, which is not a legal node in the network, can flood hello apply for any legitimate node using high transmission power and break the security of WSNs. In this variety of attack an attacker with a high radio transmission range and dispensation power sends Hello packets to a number of sensor nodes which are inaccessible in a large area within a WSN. The sensors are thus convinced that the competitor is their neighbor.

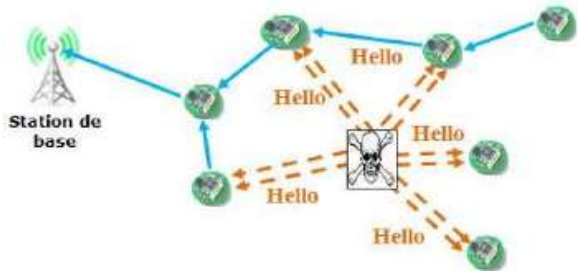

Fig 1.3 Hello Flood Attack

As a result, while transferring the information to the base station, the victim nodes try to go during the invader as they know that it is their neighbor and are ultimately spoofed by the attacker.

Wormhole Attack: Worm Hole attack is a dangerous attack in which the invader records the packets at one position in the network and tunnels those to another place. The tunneling or retransmitting of bits could be done selectively. Worm hole attack is a major threat to Wireless Sensor Networks, because this sort of attack does not need compromising a sensor in the network rather, it could be performed even at the
primary stage when the sensors start to realize the adjacent information.

Wireless Local Area Network: Wireless LAN is a connections network that provides connectivity to wireless devices within a restricted geographic area. "Wi-Fi" is the global standard for Wireless Networks and is the wireless comparable of wired Ethernet networks. In the office, Wi-Fi networks are attachment to the wired networks.

Fig 1.4 Wireless local area network

At home, a Wi-Fi network can provide as the barely network as all laptops and many printers come with Wi-Fi built in, and Wi-Fi can be added to desktop computers using USB.Wi-Fi is achieved with a wireless base location, called an "access point." Its antennas broadcast and receive a radio frequency within a range of 30 to 150 feet during walls and other barriers. Since all wireless and wired computers are interrelated, they can exchange data with each other for backup and file sharing. For details of the wireless principles. See Wi-Fi hotspot, cellular hotspot , router , LAN switch , wireless broadband and WPAN.

CONCLUSION

Provision of protection in network is a essential requirement for sufficient and stable network in communication technologies. It is a multifarious feature to deploy in wireless sensor network because due to the nature of network. The most physical security attacks concern the WSN security dimensions like confidentiality, integrity, validity and availability. In this short review, The security issues and physical attacks analyzed. We try to axis more specific knowledge for researchers. The approach is to classify and compare the WSN's physical attack, their properties such as their strategies and effects and finally their associated recognition and distrustful techniques against these attacks to handle them separately and extensively.

REFERENCES

[1] Shio Kumar Singh, M P Singh D K Singh "Routing Protocols in Wireless Sensor Networks – A Survey " International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010
[2] Mark A. Perillo and Wendi B. Heinzelman, Wireless Sensor Network Protocols.
[3] Aamir Shaikh and Siraj PathanResearch on Wireless Sensor Network Technology International Journal of Information and Education Technology, Vol. 2, No. 5, October 2012.
[4] Edwin Prem Kumar Gilbert, Baskaran Kaliaperumal, and Elijah Blessing RajsinghResearch Issues in Wireless Sensor Network Applications: A Survey , International Journal of Information and Electronics Engineering, Vol. 2, No. 5, September 2012
[5] Eiko Yoneki, Jean Bacon," A survey of Wireless Sensor Network technologies: research trends and middleware's role 2005 Eiko Yoneki, Jean Bacon Technical reports published by the
[6] Sandra Kay Miller ― Facing the Challenge of Wireless Security‖ July 2001.
[7] Goldsmith, Colin, (2004). Wireless Local Area Networking For Device Monitoring,Master thesis, University of Rochester Rochester, New York.
[8] IEEE Standard for Information technology— elecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
[9] H. Wu, Y. Peng, K. Long, S. Cheng and J. Ma, "Performance of reliable transport protocol over IEEE 802.11 wireless LAN: analysis and enhancement," INFOCOM 2002. 21st Annual Joint Conference of the IEEE Computer and Communicatio ns Societies. Proceedings. IEEE,Vol. 2 Isssue 2002, pp. 599-607 07 November 2002.

[10] Q. Cao, T. Li, Tianji and D. Leith "Achieving fairness in Lossy 802.11e wireless multi-hop Mesh networks",In: Third IEEE International Workshop on Enabling Technologies and Standards for Wireless Mesh Networking MESH, Macau SAR, P.R. China pp. 1-7, 2009.
[11] Nikita Borisov, Ian Goldberg and David Wagner. "Intercepting Mobile Communications: The insecurity of IEEE802.11", 7th Annual International Conference on Mobile Computing and Networking. July 2001.
[12] IEEE Standard for local and metropolitan area networks, "Port-based Network Access Control" , IEEE Std 802.1x, 2001 Edition (R2004).
[13] IEEE Standard for local and metropolitan area networks , "Wireless LAN Medium Access Control (MAC) and Physical Layer pecifications, Medium Access Control (MAC) Security Enhancements". ANSI/IEEE Std 802.11i, 2004 Edition.
[14] Tom Karygiannis and Les Owens, " Wireless Network Security: 802.11, Bluetooth and Handheld Devices", National Institute of tandard and Technology. November 2002.