IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 3, Issue 1, Feb-Mar, 2015
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Review of Security Attacks and Issues in Wireless Sensor Network

Mohammad Ziaullah[1], Roshan Ara[2], Prakash Shetty[3]

[1]Department of Digital Communication And Networking, P A College of Engineering, Mangalore, Karnataka, India

[2]Department of Digital Communication And Networking, DR P.G Halakatti college of Enginnering, Bijapur, Karnataka, India

[3]Department of Electronics And Communication Engineering, P A College of Engineering, Mangalore, Karnataka, India

Abstract

Wireless sensor network is one of the most growing technology for sensing and performing the different tasks. Such networks are beneficial in many fields, such as emergencies, health monitoring, environmental control, military, industries and these networks prone to malicious users' and physical attacks due to radio range of network, un-trusted transmission, unattended nature and get access easily. Security is a fundamental requirement for these networks. In this paper, our center of attention is on physical attacks and issues in wireless sensor networks. Through this review, easily identify the purpose and capabilities of the attackers. Further, we discuss well-known approaches of security detection against physical attacks.

Keywords: *Wireless sensor network, physical attacks, security detection, malicious.*

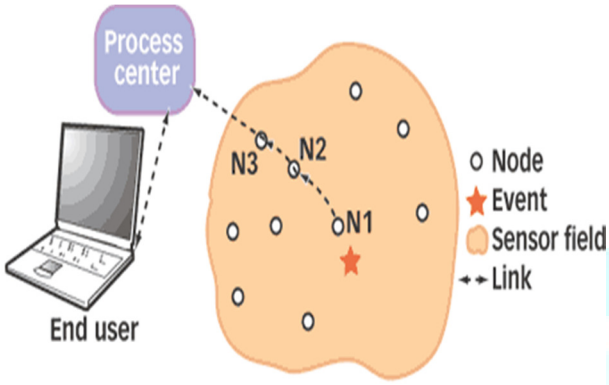
1. Introduction

The nature of heterogeneous systems and with many potential applications wireless sensor networks garnered a great deal of attention by researchers. The wireless networks contain hundred or thousand tiny and low cost; low power and self organize sensor nodes perform their functions in network. The sensor nodes are highly distributed inside the system. The sensors nodes are used for monitoring different environments in the cooperative manner and compute the data for analyzing. The two components of wireless sensor network aggregation and base station, aggregation collect the information from there nearby sensors, integrate them and send to the base station for processing. The wireless sensor network nature of communication is unprotected and unsafe because of deployment in hostile environment, limited resources, an automated nature and untrusted broadcast transmission media. The most of security techniques are not sufficient in WSN network and security is a vital requirement for network. The main objective of this paper is to review different security dimensions of wireless networks such as integrity, confidentiality, authenticity and availability. Further, overview on physical attacks on WSN and discuss security issues

Overview of WSN: The WSN is based on the dense deployment of disposable low energy, low cost tiny nodes for gathering real time information. Common functions of WSN are broadcasting, multicasting and routing. These nodes consist of three major components sensing, processing and communication. Various types of sensor network play a significant role in the different field. In terrestrial wireless sensor network nodes are dispersed and randomly or pre-planned manner placed into the target area. The battery power is limited in these networks. Another type is underground WSNs, in this type the nodes are buried underground like cave or mine for monitoring the conditions. The nodes are expensive in this type compare to terrestrial type. The multimedia sensor network has low cost nodes and equipped with microphones and cameras. This type of network needs more bandwidth and high energy and quality of service for processing the data. The underwater sensor networks are located underwater for gathering the data and network nature is sparse. The signal fading, delay and long propagation are main issues in this networks [1].

The wireless sensor network were primarily proposed in domains where wired networks are not

suitable and infrastructure missing. The hundred and thousand nodes are needed to achieve the assigned task such as are military applications, shown in Figure 1.



1. This illustration shows a simple wireless sensor network (WSN).

Fig. 1: Application of WSN

Security in WSN: Security is one of the main characteristic of any system and traditional wireless sensor network affected with many types of attacks. The security attacks concern for WSN because of physical accessibility of sensor and actuator devices in network and usage of minimal capacity in a network. These weaknesses or security attacks still present in WSN and can be handled using various security architectures and security services like integrity and authenticity, confidentiality in the wireless domain [3].

Security Issues in WSN

Availability: The availability in wireless sensor network ensures the network services are feasible even in the subsistence of denial of service attacks. The securities protocols perform the availability of data in the network with fixate low energy and storage with reuse of code in network [4]. In availability, a few approaches choose to adjust the code to reuse as much code as possible and make use of extra communication to achieve the same goal.

Self Organization: The wireless sensor network has many nodes for operations and deployed in different locations and fields. In self- organization, the nodes are flexible to be self-organizing and self -healing in network. The WSN is an Ad hoc network and all nodes are independent in network and without infrastructure. This intrinsic characteristic brings a great challenge for wireless network and security, as well.

Time Synchronization: The wireless sensor network applications rely on some type of synchronization. The nodes have two states in the network on and sleep and radio may be turn on or in sleep mode for period of time. The sensor calculates the end-to-end delay of a packet [5].

Secure Localization: Wireless sensor network use location based information for identifying the position of nodes in the network. Few attacks are related with sensor location by investigating for attacks. The attackers are searching the header of packet and data for this purpose. The secure localization is an important factor during implementing security in the network.

Confidentiality: The confidentiality is restricted data access to authorized personnel. The data should not leak across adjacent sensor network. When one node sends the highly sensitive data to the destination, it passes from many nodes in the network. For the provision of security in data, network protocols are using encryption technique with a secret key, the message is sent in encrypted for to the channel. Information should encrypt to protect from traffic analysis attack [6].

Authenticity: Authenticity is imperative in WSN, because an adversary can easily inject messages. The receiver node need to guarantee that data used in any decision making process originate with trusted source. The data authenticity is to ensure of identities of communication nodes. It is required in various administration tasks [4].

Flexibility: The sensor network scenarios are different and depending on environmental conditions, hazards and mission because they are changing frequently [5]. The changing mission goals frequently need sensors to be reduced from settle nodes in the network.

Physical Attacks: A wireless sensor network is designed in layers form and these layers protect the sensor with various attacks as shown in Figure 2. The sensor networks are power constraint with a limited computational power, because of these characteristics exposed the network for attackers. The physical attacks based on different strategies and effects. Below we

discuss physical attacks in detail.

Signal Jamming Attack: The signal or radio jamming attack is transmit the radio signals emitted by the receiving antenna at the same transmitter. The attack techniques are constant, deceptive, random and reactive jamming in this attack. These attacks effects on radio interference and resource exhaustion. The attack is based on modification class and always the availability integrity is a main threat for WSN in this attack. It is belong to external and active threat model. The detection of this attack possible through detecting background noise and

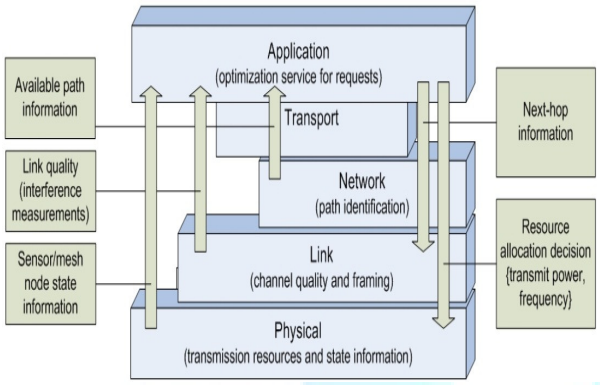


Fig. 2: Security in wireless sensor networks layers model

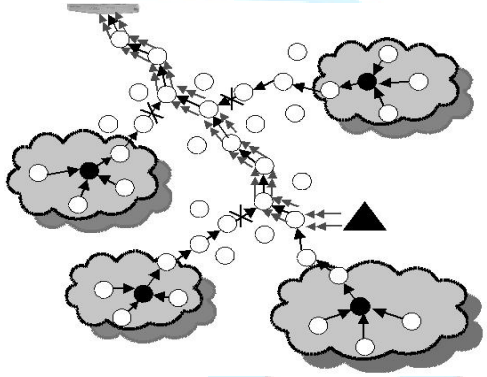


Fig. 3: Path Based DOS Attack in end-to-end Communication [8]

misbehavior detection techniques. Another detection method is statistical information and channel utility degradation than a threshold. The WSN network has some defensive approaches to protect from these attacks such as encryption approach, access restriction, buffering, reporting attacks to base station and through mapping protocols.

Tempering and Capturing Attack: Another physical attack is device-tempering attack on network; the attacker captured the sensor node physically and replaces the node with their malicious node. The effects of this attack are stopping the services or disturb the network and may control over the captured node [7]. This attack belongs to intersection, modification and fabrication security class. The availability, integrity and confidentiality are the attack threat in this class. The detection of this type of attack possible through sensor node disconnection, node destruction and notice misbehavior of the node in network. The defensive mechanism is optimizing and using crypto-processors and applying standard precautions in network. Further the physical protection of node and malicious node detection techniques are protect the network from these attacks.

Path Based DOS Attack: The path based DOS attack is another category of physical attaches and typically, combination of jamming attack. In this attack, the attacker sends a large number of packets to the base station. The effects of this physical attack are disturbing the network availability and node batteries exhaustion. The path based DOS attack is belonged to modification and fabrication class and availability and authenticity are main threats for WSN network. In below Figure 2 shows the nodes affected by path based DOS attack. Initially the nodes along the path will rapidly become exhausted and after this the second nodes downstream from nodes along the main path and unable to communicate with base station. This is because of tree-structured topology and in last; the path based DOS attacks can disable a much wider region than simply a single path.

Node Outage Attack: The node outage attack is stopping the functionality of WSN components 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. The attack is belong to modification model and availability and authenticities are main threats for this attack in network.

Eavesdropping Attack: The eavesdropping is a

detection of contents of communication by overhearing attempt to data and apply through WSN transmission medium. The eavesdropping is also called confidentiality and lead to wormhole or blackhole attacks in network [9]. The effects of this attack are extracting sensitive WSN information and delete the privacy and confidentiality of nodes. The attack is belongs to intersection model and confidentiality is a main threat in network for this attack and based on external and passive threat models.

DOS (Denial of Services) Attack: The DOS attack is a general attack and applies on layers such as data link layer, network layer and transport layer etc. In this attack, the attacker can inject fake broadcast packets to force sensor node to perform expensive signature verification. The DOS attack effects the layers and their functions in network. The DOS attack is belongs to interruption and intersection security class and availability, integrity and authenticity are main threats for this attack [10].

CONCLUSION

Provision of security in network is a vital requirement for sufficient and stable network in communication technologies. It is a complex feature to deploy in wireless sensor network because due to the nature of network. The most physical security attacks disturb the WSN security dimensions like confidentiality, integrity,authenticity and availability. In this short review, the security issues and physical attacks analyzed. We try to focus more specific knowledge for researchers. The approach is to classify and compare the WSN's physical attacks, their properties such as their strategies and effects and finally their associated detection and defensive techniques against these attacks to handle them independently and comprehensively.

4. Jain, M.K., 2011. Wireless sensor networks: Security issues and challenges. International Journal of Computer and Information Technology, 2(1): 62-67.

REFERENCES

1. Lewis, F.L., 2004. Wireless sensor networks. Smart environments: technologies, protocols and applications, pp: 11-46.
2. Haboub, R. and M. Ouzzif, 2011. Secure Routing IN WSN. International Journal, pp: 2.
3. Giruka, V.C., *et al.*, 2008. Security in wireless sensor networks. Wireless communications and mobile computing, 8(1): 1-24.
4. 5.. Pooja, M. and D.Y. Singh, 2013. Security Issues and Sybil Attack in Wireless Sensor Networks. International Journal of P2P Network Trends and Technology, 3(1): 7-13.
6. Singh, S.K., M. Singh and D. Singhtise, 2011. A survey on network security and attack defense mechanism for wireless sensor networks. Int. J. Comput. Trends Tech, pp: 5-6.
7. Becher, A., Z. Benenson and M. Dornseif, 2006. Tampering with motes: Real-world physical attacks on wireless sensor networks. Springer.
8. Deng, J., R. Han and S. Mishra, 2005. Defending against path-based DoS attacks in wireless sensor networks. in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. ACM.
9. Kalita, H.K. and A. Kar, 2009. Wireless sensor network security analysis. International Journal of Next-Generation Networks (IJNGN), 1(1): 1-10.
10. Ning, P., A. Liu and W. Du, 2008. Mitigating DoS attacks against broadcast authentication in wireless sensor networks. ACM Transactions on Sensor Networks (TOSN),