RESEARCH REVIEW JOURNALS
Volume-04
Issue-05
May-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Wireless Sensor Networks: A Study on Security Goals and Issues

[1] Raj Kumar & [2]Dr. Kirti Walia

[1]*Research Scholar, RIMT University, Mandi Gobindgarh Punjab (India)*
[2]*Professor, RIMT University, Mandi Gobindgarh Punjab (India)*

ARTICLE DETAILS

Article History
Published Online: 25 May 2019

Keywords
Wireless sensor networks, security attacks, security goals.

***Corresponding Author**
Email: krishna268[at]gmail.com

ABSTRACT

Wireless Sensor Networks (WSN) is a most rising technologies and it is also a challenging research domains in today's' era. A wide range of applications used in WSN's like, education military, health, agriculture, industry/business and environment etc. The WSN technology is highly faced with the issues of network and functional security of natural limits in energy and computing power. The attacks may affect on any hardware or software to damages these networks. These networks produce most recent security threats in contrast to conventional techniques, due to various excellent features of the networks. There are numerous security goals in the networks and these goals must be kept in mind while designing of security solutions for these networks In this study, we have covered a variety of security attacks like Jamming, Hello, Sybil, DoS,, & selective forwarding attack and further, we focused on other security issues of wireless sensor networks and its countermeasures.

1. Introduction

A WSN is a disciplined network and all wireless sensor equipment is identifying as sensor node & every node is connected with one to many other sensor nodes. The main aim of a wireless sensor network is to gather information from the physical world and they monitor the physical or environmental state such as sound, temperature, pressure, vibrations or pollutants and communicate data through the network accordingly. The sensors used in these networks collect data, process the data and pass the data through the central node, they are beneficial in the environments and infrastructures where wires are not suitable. In today's' world most of the application are working through WSNs which stimulate the researcher/scientists to make efforts on other issues connected to WSN security attacks. At all security networks include the features of privacy, integrity authorization and authentication. To execute security system depends on different constraints like a number of sensors range, power and its deployments are major challenges in WSN. Further the different security attacks like against WSNs, we have covered in this paper.

2. Security Goals of Wireless Sensor Networks

A variety of Sensor networks are distributed networks and they share different commonalities with a classic computer network Therefore security goals of WSN includes both typical & special network requirements must contains attributes such as confidentiality, integrity, data freshness, availability, and authentication of WSNs. The major security goals of Wireless Sensor networks are described below .

2.1 Data availability :

- It ensures that services and information can be accessed at that time that when they are required.
- Data must be available for operational network.
- To move the packets network services should be available.
- To develop the various resources nodes should be competent.

2.2 Data authentication :

- It ensures the uniformity of the message by identifying its source
- Its objectives are necessary to achieved when clustering of nodes is performed.
- Data authentication is the ability to receiver and verifies the data received from correct sender.
- In two way communications the sender and the receiver share a secret key to compute through Message Authentication Code (MAC) of all communicated data

2.3 Data freshness :

- Data freshness ensures that message is recent, where the old message is not reuse
- To attain data freshness network procedures must be planned in a system to recognize duplicate packets and throw away them to stop possible mix-up.
- Fresh data verify that data is fresh and no previous information has been repeated.
- Timestamp can be utilize to ensure that information/packets are fresh..

2.4 Data Integrity

- It is a service which promises that information are not be modified during the transmission.
- It defends the network against the alteration of communications.
- It ensures and confirms the consistency of data will not tamper.
- Data privacy refers to protection of informations from harmful nodes.

2.5 Self-Organization :

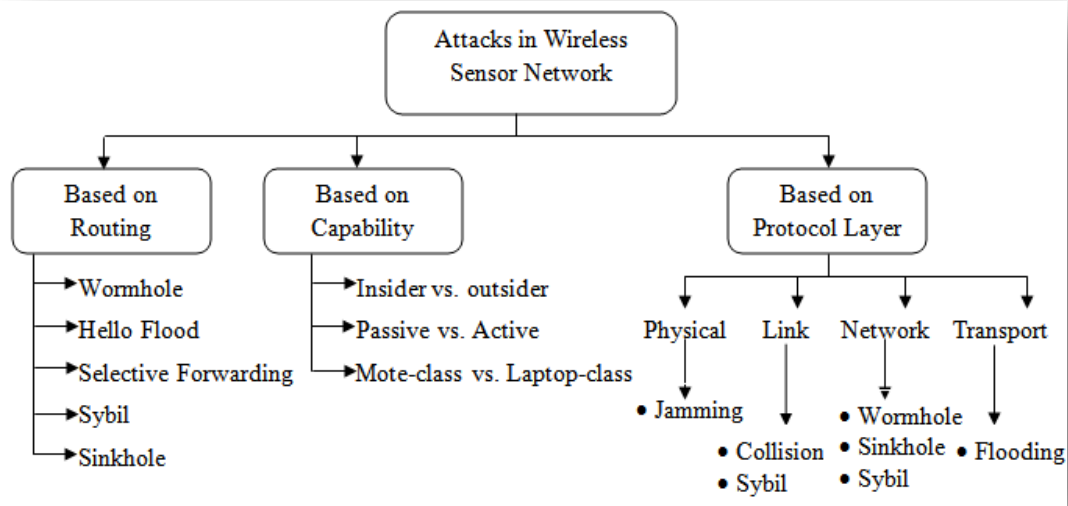
- WSNs various nodes for operation can be installed on different locations.
- In self organization the nodes are easy to move to self-healing in network
- WSN is ad hoc network and each node is self-determining in the network.

2.6 Time Synchronization :

- The WSNs calculate the uninterrupted stay of a packet.
- The sensor network applications are depend on time synchronization.
- The WSNs may require set of synchronization for tracking more applications.

3. Attacks in Wireless Sensor Networks

In regards to security threats the basic networking protocols and sole characteristics are completely helpless. Attacks can take place at any level such as active and passive attacks. The majority of routing protocols have not planned and designed the security systems that's why attackers can break the security networks smoothly, for example jamming, tampering, exhaustion and collisions and many more attacks etc. A diversity of attacks against WSNs is acknowledged and its countermeasures are also covered in this section.



3.1 Wormhole attack : In wormhole attack, attacker pressure the sender and receiver nodes when they are located at distance of one to two steps but genuinely this distance have multiple steps & typically both are out of range. Normally selective forwarding and wormhole attacks are used in combination. It incarcerates the data/information at one spot and repeats them at different spot either unaffected or fiddled. If wormhole attack used in combination with Sybil attack then detection of attack is more difficult.

3.2 Hello Attack : In this attack, when attacker with high transmission power can throw or repeat hello packets which are used for neighbour detection. The attacker generates an false impression of being neighbor to further nodes and primary routing protocol can be disturb which help additional style of attacks. This attack is one of the least complicated attacks in wireless sensor networks. Therefore energy gets exhausted as nodes seek to send messages to receiver that is away from their frequency scope.

3.3 Selective Forwarding : It is a very dangerous attack against wireless sensor networks which can change the entire sensor network communication.

3.4 Sybil attack . This attack regularly objects fault tolerant ideas including distributed storage, topology maintenance, and multi-hop routing. It is a single attacker that presents and creates different characters to other nodes in wireless sensor networks. The sybil attack is normally used to harass several types of protocols. It is a location based serious threats which exchanged the location information by efficient routing protocols.

3.5 Inside and Outside attack (laptop-class / Mote-class attacks) :In this attack the attackers have at least one authorized node in the network to steal the key/code. It is also known as insider attack (mote-class attack). Secondly, in the outside attack the attacker does not have any particular access to the network is called outside attack. Another attack where attacker can access more helpful controlling devices having additional battery power, more competent CPU, vigorous radio communication and sensitive antenna etc., are also known as laptop-class attacks.

3.6 Jamming : In this attack, the attacker interfaces with communication frequencies and it include various types of jamming attacks.

- Jam signals transmitted when traffic is sensed is called reactive jamming,
- It corrupts the packets when jamming attack work constantly.

- A flow of information in the network is fraudulent transfer through jamming attack.

3.7 Exhaustion and collisions attacks : In this attack the attacker can miss their transmission time on the further nodes. Due to this confusion can create in the performance of the network**.** This is known as unfairness.

3.8 Tampering : Tempering is easy to perform but pretty harmful. In this attack, the attacker may access physically modifying and destroying the sensor nodes. In other word it is called node capturing in which node is conciliation. This attack creates a threat to the availability, integrity and confidentiality of the data.

3.9 Denial of Service (DoS) attack: In this attack, fake packets are injected by the attackers that affecting the availability, integrity and authenticity of the data. This attack can be applied in all the network layers such as data link, network and transport layer etc.

3.10 Cloning Attack : It is most difficult problem in WSN security. In this attack, attacker crack the sensor nodes, terminate it and introduce various copies of the node back into sensor network. Cloning provide the easy way to attacker to create mischievous nodes which can damage the sensor network

3.11 Spoofing : In this attack the attacker can transform the routing protocol information. They can also generate routing loops and false messages etc. This is known as spoofing of routing information.

Security for counter measures on wireless sensor networks

Jamming	It can be prohibited by various techniques like • Eavesdropping • message modification • message repeat attacks • strong encryption techniques • and time stamps are to be used
Hello	It can be prevented if every node in the network authenticates to neighboring nodes by identity and verify the protocols on trust base stations
DOS	To prevent DoS attacks consist, payment network resources, pushback, strong authentication and identification of networks.
Sybil	It can be prevented by efficient protocols for gateways or base stations. The detection of Sybil attack is not simple in wireless network but with the help of radio resource testing it can be used to detect its occurrence in the networks.
Warmhole	This attack can be identify and prevented through packet leashes method by using geographic and temporal information
Selective forward	It can be prevented by utilizing multipath routing protocols

4. Conclusion

The wireless sensor networks are growing with rapid speed in technology world. The need of WSN applications in all the fields where sensor networks are required to perform. Due to security and dependability of such networks is highest significance and has become the issue of major distress. In this paper, we have discussed various security issues and attacks in wireless sensor networks. Further, we have also covered various security mechanisms to prevent from these attacks. Since wireless networks are more susceptible to attacks, thus, there is a strong need to design efficient and more robust security mechanisms to make wireless networks more secure so that the data in such networks should be handled with full confidentiality and high security.

References

[1] A.K. Nuristani and Jawahar Thakur, “Security Issues and Comparative Analysis of Security Protocols in Wireless Sensor Networks: A Review “Security Issues and Comparative Analysis of Security Protocols in Wireless Sensor Networks: A Review Vol.6, Issue.10, Oct. 2018 E-ISSN: 2347-2693

[2] Priyanka Sharma, “Overview of Security Mechanisms and Attacks in Wireless Sensor Networks” International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Volume 6 Issue 1, January 2017

[3] Pooja and Dr. R.K.Chauhan, “Review on Security attacks and Countermeasures in Wireless Sensor Networks” International Journal of Advanced Research in Computer Science. Volume 8, No. 5, May-June 2017.

[4] Rutuja Jadhav and Vatsala, “ Security Issues and Solutions in Wireless Sensor Networks” International Journal of Computer Applications (0975 – 8887) International Journal of Computer Applications (0975 – 8887)

[5] A.S.K. Pathan, Hyung-Woo Lee; C.S. Hong, “Security in Wireless sensor networks: issues and challenges”, Advanced Communication technology, IEEE Xplore

[6] C. Karlof, D. Wagner, “Secure Routing in wireless sensor networks: attacks and countermeasures”, Elsevier, Vol. 1, Issues 2-3, pp. 293-315

[7] KehinaChelli, “Security Issues in Wireless Sensor Networks: Attacks and Countermeasures”, Proceedings of the World Congress on Engineering 2015, Vol 1, London, UK.
[8] K. Shabana, N. Fida, F. Khan, S.R. Jan, M.U.Rehman, “Security Issues and Attacks in Wireless Sensor networks”, IJARCSEE, Vol. 5, Issue 7, July 2016.
[9] Prasad Mahajan, Priyanka Bhute. A Survey of Wireless Sensor Network Security, International Journal of Advanced Research in Computer and Communication Engineering
[10] Mulla RI, Patil R (2016) Review of attacks on wireless sensor network and their classification and security. Imperial J Interdiscipl Res 7: 2.
[11] Genita Gautam, Biswaraj Sen, “Survey on different types of Security Threats on Wireless Sensor Networks,” International Journal of Computer Science and Information Technologies, Vol. 6, 2015
[12] Kanchan Kaushal and Taranvir Kaur, “A Survey on Attacks of WSN and their Security Mechanisms,” International Journal of Computer Applications, Volume 118, No. 18, May 2015.
[13] Neha rang , Anuj gupta , “ Wireless Sensor Networks : A Overview”, IJMCS, Vol.1,iss.2, 2013
[14] Aashima singla , Ritika sachdeva , “ Review on security issues and attacks in Wireless sensor networks”, IJARCSSE, vol. 3, iss. 4, 2013
[15] L. kaur and J. Malhotra, "Review on Security Issues and Attacks in Wireless SensorNetworks", International Journal of Future Generation Communication and Networking Vol. 8, No. 4 (2015), pp. 81 -88.
[16] R. W. Anwar, M. Bakhtiari, A. Zainal, A. Hanan Abdullah and K. N. Qureshi, "Security Issues and Attacks in Wireless Sensor Network", World Applied Sciences Journal 30 (10), 2014.
[17] M. A. Jan, P. Nanda, X. He, and R. P. Liu, “A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application,” Elsevier Future Generation Computer Systems (FGCS), “Accepted”, 2016.
[18] Hosein Marzi, Arash Marzi, "A security model for wireless sensor networks", 2014 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), Ottawa, ON, pp. 64-69, 2014.
[19] Jyoti Ahlawat, Mukesh Chawla and Kavita Sharma, “Attacks and Countermeasures in Wireless Sensor Network”, International Journal of Computer Science and Communication Engineering (IJCSCE), pp. 66-69. 2012
[20] M. U. Aftab, O. Ashraf, M. Irfan, M. Majid, A. Nisar and M. A. Habib, “A Review Study of Wireless Sensor Networks and Its Security”, Communications and Network, Vol. 7, No.4, pp.172-179, 2015

