International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Overview of Security Mechanisms and Attacks in Wireless Sensor Networks

Priyanka Sharma

GCET, Greater Noida, India

Abstract: ***WSN technology is expanding day by day. The WSN technologies which are related to network protocol have been structured for the efficiency of energy. This paper is used for examining security mechanisms which are designed for application and network layers. Wireless Sensor Networks (WSNs) are recruited in several regions in a variety of claims named as fitness, ecology, and service; for example, to rule the chief data such as the location of staff in a building for this type of example WSNs security is required. WSN which are cluster-based gives finer hold up, functionality, benefits, and output in plenty of applications, by which numerous routing protocols which are cluster based have been evolved in WSN.***

Keywords: Wireless sensor networks, Security, applications, WSN, attacks, routing protocols

1. Introduction

WSN contains an arrangement of sensors. In which every sensor network node consists numerous segments: a radio, antenna, microcontroller and transceiver [1]. A Base station that is used to publicize the information that is used for processing connects the sensor network with another network. Utilization of power is one of the considerable disadvantages in sensor network [3]. The WSN gives permission to sensors to communicate with the ad-hoc network for linking these sensors back to a Base Station which are used for solving the problem of individuals in a network and which acts as a gateway. WSNs can also be used for designing and operating purpose by the help of which uncomplicated designs are evolved and can also be used to examine the surroundings without any wired networks. In this security should be the major concern because of which many sensor networks owns a variety of complicated duty and for which security is required. There are several applications of wireless sensor networks which are used for examine, analyzing and scanning [5]. The designing of a routing protocol is the chief constraint in WSNs with restricted power of sensor nodes that is used for making the communication protocol with efficient energy [2]. The routing approach includes Cluster Based Routing (CBR) scheme which is one of the most used schemes in static and mobile WSN. Sensors are divided into a variety of clusters in this type of routing in which every cluster include Cluster Head (CH) which is used for gathering information in its cluster from every member nodes.

Figure 1: Model of WSN threats

2. Security Requirement

For making the WSN communication method secure several security requirements are needed which are illustrated as follows:

2.1 Confidentiality

To keep the information private and within an individual, this security service is used. Confidentiality is one of the most important methods used in security service.

2.2 Authenticity

This is used for keeping the communicating nodes specification private. In this, each node is verified again and again in transmission method [17]. For security purpose, in this authentication code is generated so that no data or information is a steal.

2.3 Integrity

Integrity is used for securing the message during the transmission time. So that attacker cannot steal or change the communicated messages. In this cyclic redundancy checksum (CRC) method is used for scanning the errors.

2.4 Availability

In this attackers can enable attacks by which network performance is reduced or abrupt the whole network [4]. The denial of service is one of the injurious network availability.

2.5 Survivability

In this type of service limited amount of space is given.

2.6 Privacy

Privacy is one of the vitally used security requirement which is used for make sure that data reaches to only its sanction entity [7].

2.7 Time synchronization

Time synchronization is used in several applications of sensor networks which use synchronization of time.

Figure 2: Security requirements in WSN

3. Constraints in Wireless Sensor Network

A WSN is made up of enlarging sensor nodes which are resource-constrained devices [11]. These nodes have restricted the power of processing data, less volume for keeping data, and constrained bandwidth of communication. These constraints are because of its restricted energy and fleshly size of the sensor nodes [15]. Due which it is hard, to engage the security mechanisms in WSNs. The major constraints used in WSN are as follows:

3.1 Energy Constraints

Energy is the chief constraint used in WSN. The utilization of energy is partitioned into three segments: (i) energy used in transducer of sensor, (ii) energy used for transmission purpose, and (iii) energy used for microprocessor computation [16]. It is studied that each time transmission in WSN cost same power which is used for executing 800 to 1000 instructions. Thus, computation is cheaper than communication in WSNs. WSNs are categorized in several levels of security which rely on energy cost.

3.2 Memory Restrictions

A sensor contains less space for storage and uses less amount of memory. A sensor node is a memory which contains flash memory and RAM. In this downloaded application code is stored in flash memory and application program is stored in RAM. In this, it is difficult to run complex algorithms because there is no plenty space is left to run algorithms after loading the application code and OS.

3.3 Unreliable Communication

It is one of the major threats to the security of sensor. In this connectionless protocols are used on which packet-based routing of sensor networks relies. Because of channel errors packets get damaged or congested nodes get dropped [18]. It may also escort to affected packets. In many circumstances, if the channel is reliable, then it is not necessary that the communication is also reliable. This is because when packets retransmit then each time they collide with each other this situation takes place.

3.4 Higher Latency in transmission

The major cause which leads to higher latency transmission in a packet transmission includes multi-hop routing, network congestion and dealing with intermediate nodes in WSN. Because of which it is hard to attain synchronization [6]. For safety purpose synchronization is the chief concern as some mechanism depends on cryptographic key distribution and critical event reports.

3.5 The neglected operation of networks

In some methods, the nodes are positioned in remote areas that are neglected in WSN. Because of such surroundings sensor confronts a bodily attack which is high.

4. Challenges in WSN

A WSN consists of many challenges which are described below:

1) Resource restriction is used for holding systematic utilization of resources viz. energy aware routing etc.
2) Supreme surrounding and dynamic situations are used for holding adaptive network operation.
3) For removing redundancy of data, it is important to implement fusion of data and localized sorting techniques. In some applications, data aggregation experiments that focused in average, maximum or minimum values [10]. In such methods, all the sensed

data is not transmitted by sensor nodes, since for some immediate sorting the sampled data which are aggregated by the node is produced in an interval of time and after that only Final data which is required for transmission can be used for communication reduction.

4) Reliability studies and reliability mechanisms are used for holding non authentic wireless transmission.
5) Data-centric transmission paradigm is used for focusing on produced data by a group of sensors can only be used for holding non global identification for sensor nodes [9].
6) Fault tolerance is used for eliminating the crash of non-awaited node failures.

5. Attacks on WSN

Security is the chief concern in WSN. In many methods, nodes are positioned in located in a hazardous environment. In such situation their physical safety is in danger and as an outcome WSN have shielded susceptibility.

5.1 Denial of Service (DoS)

Denial of Service is caused by hostile activity. By sending more unnecessary packets, the DoS attack which is an easiest one can easily utilizes all the resources that are achievable to the sufferer node. As an outcome, it obstructs individuals in a network from obtaining services from which this attack is calculated to demolish and minimize the set up of a network [17]. Dos attacks are used and presented in all the layers and each layer has different roles for example in physical layer this attack is used for tampering and jamming purpose. In link layer, it is used for crashing and weakness purpose. In network layer, they could be unattended, directionless and homing and in transport layer, it could be poisonous flooding and DE synchronization.

5.2 Wormhole attack

In this attacker, reply over a network in which Low latency connection between two parts contain messages which are a wormhole [8]. Direct node accepts this types of link and direct the messages between two non neighboring nodes which are adjacent to each other, or by a pair of nodes which are in different segments in a network so that they can communicate with each other. Both sinkhole and wormhole attack have alike functions.

5.3 Hello flood Attack

It is one of the easiest attacks from all of the above, in which attacker sends the message like HELLO to both sender and receiver with great capacity and power. The receiving nodes think that the node, which sends the message to them is the nearest node to them and they also send the packets to them [14]. Congestion is the main problem which occurs by this attack in the network which is one of the DOS attacks. In this attack blocking methods are used to secure Hello Flood attacks [12].

5.4 Sinkhole attacks

The main aim of this attack is to convince all the traffic from a special network by compromising a node and making a hole at the base station [13]. This compromising hole takes interest in routing algorithms in which this attack can act. Since the information provided by the node contain difficulty. This type of attack is hard to counter.

5.5 Sybil attack

This type of attack defines a circumstance in which an identity of the network displays higher. This type of attack easily comes under the influence of the fault-tolerant plans, storage allocation and topology of network which are protocols and algorithms [9]. One of the examples is a plan of distributed storage. There are three categories which are a replica of this type of data evolved. It contains three nodes in which compromised node is one of the two nodes can easily minimize the redundancy.

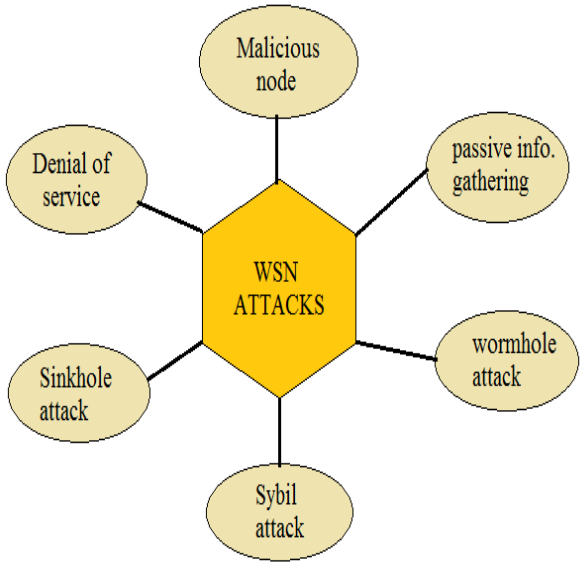

Figure 3: Attacks in WSN

6. Conclusion

During the evolvement of WSNs, the request for security in becomes clear. It includes many restrictions which are stated as the limited amount of energy, processing of data, and storing volume. In this paper, many constraints, challenges, attacks, and security mechanism have discussed. The security becomes the chief concern in WSN as because of these attacks found in WSN for avoiding this several mechanisms have been evolved which are data confidentiality, privacy time synchronization and much more discussed in this paper. Although in past there was not many mechanisms to provide protection. But nowadays several solutions are there for avoiding any dangerous activity. These types of mechanism make WSN different from other networks. Many methods and protocols have been evolved in this network.

References

[1] Neha rang , Anuj gupta , " Wireless Sensor Networks : A Overview", IJMCS, Vol.1,iss.2, 2013.
[2] C. Karlof , D. Wagner , " Secure routing in wireless sensor networks : attacks And countermeasures", In proc. Of the 1st IEEE Int. workshop on sensor network

Protocols and applications (SNPA'03) , pp. 113-127, May 2003.
[3] Aashima singla , Ritika sachdeva , " Review on security issues and attacks in Wireless sensor networks", IJARCSSE, vol. 3, iss. 4, 2013.
[4] Kriti Jain, Upasana Bahuguna, "Survey on Wireless Sensor Network", IJSTM, Vol. 3, Issue 2, pp. 83-90, Sept 2012.
[5] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", IJCIT, vol. 2, issue 1, pp. 62- 67, 2011
[6] Tin win maw,Myo hein jaw, " A secure for mitigation of DoS attack in cluster Based wireless sensor networks", IJCCER , vol. 1,Issue 3,2013
[7] Prajeet Sharma, Niresh Sharma, Rajdeep Singh, "A Secure Intrusion detection System against DDOS attack in Wireless Mobile Ad-hoc Network",IJCA, Vol. 41–No.21, March 2012.
[8] Snehlata Yadav, Kamlesh Gupta, Sanjay Silakari, "Security issues in wireless Sensor network",Journal of information system and communications,vol.1, issue 2, 2010, pp-01-06
[9] J. C. Choi and C. W. Lee, "Energy modeling for the cluster-based sensor networks," In Proceedings of the Sixth IEEE International Conference on Computer and Information Technology, pp. 218, September 20–22 2006.
[10] S. Selvakennedy and S. Sinnappan, "An energy-efficient clustering algorithm for multi-hop data gathering in wireless sensor networks," Journal of Computers, pp. 1, April 2006.
[11] Wendi B. Heinzelman, Anantha P. Chandrakasan, Hari Balakrishnan, "An Application-Specific Protocol Architecture for Wireless
[12] Microsensor Networks", IEEE Transactions On Wireless Communications, Vol. 1, No. 4, October 2002.
[13] Meena Malik, Dr. Yadhvir Singh and Anshu Arora, "Analysis of LEACH Protocol in Wireless Sensor Networks", IJARCSSE, volume 3, Issue 2, February 2013.
[14] Rajesh Patel, Sunil Pariyani, and Vijay Ukani, "Energy and Throughput Analysis of Hierarchical Routing Protocol (LEACH) for Wireless Sensor Network", IJCA, volume 20-No.4, April 2011.
[15] Ravneet Kaur, Deepika Sharma and Navdeep Kaur, "Comparative Analysis Of LEACH and its Descendant Protocols in Wireless Sensor Network", IJP2PNTT, volume 31, Issue 1, 2013.
[16] Parth M Dave and Purvang D Dalal, "Simulation and Performance Evaluation of Routing Protocols in Wireless Sensor Network", IJARCCE, volume 2, Issue 3, March 2013.
[17] V.B. Thakar, C.B Desai and S.K. Hadia, "Performance Evaluation and Improvement of LEACH- A Wireless Sensor Network Protocol using a Novel Algorithm for Clustering", Journal of Information, Knowledge and Research in Electronics and Communication Engineering.
[18] Mortaza Fahimi Khaton Abad and Mohammad Ali Jabraeil Jamali, " Modify LEACH Algorithm for Wireless Sensor Network", IJCSI, volume 8, Issue 5, No 1, September 2011.