ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Survey on Security Attack and challenges in WSN

C.Theebendra[1], S.Prema[2]

Assistant Professor, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous) Elayampalayam, Tiruchengode, India[1]

Research Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam, Tiruchengode, India[2]

ABSTRACT: Wireless sensor networks are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. Wireless sensor networks require the need for effective security mechanisms. Because sensor networks may interact with sensitive data, it is imperative that these security concerns be addressed from the beginning of the system design. WSN have a large number of constrained attached to them such as less processing capability, low memory, limited energy resources and security issues. WSN generally deployed in natural environment hence a large number of security issues are there. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. In this paper we have explored general security related issues and challenges with extensive study.

KEYWORDS: Wireless Sensor Networks, Security Attack, Issue and Challenges.

I. INTRODUCTION

A Wireless Sensor Network can be defined as a group of independent nodes, which are communicate wirelessly. Wireless Sensor Networks are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors [1][2][3]. Wireless sensors have become an excellent tool for military applications involving intrusion detection, perimeter monitoring, and information gathering and smart logistics support in an unknown deployed area. Some other applications: sensor-based personal health monitor, location detection with sensor networks and movement detection.

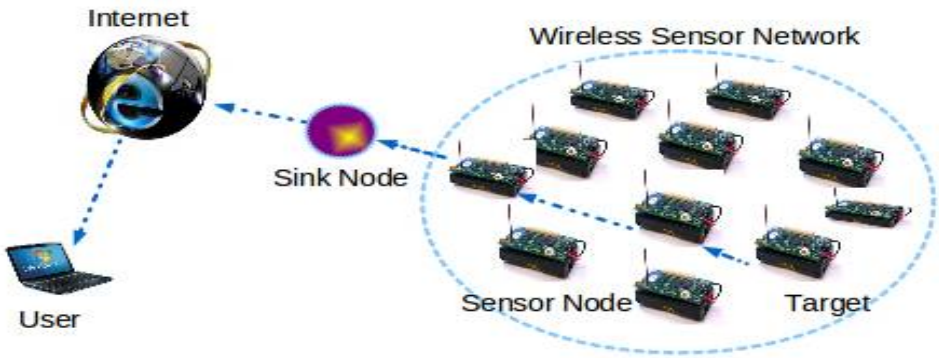

Figure 1: Wireless Sensor Network

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

In case of wireless sensor network, the communication among the sensors is done using wireless transceivers.
The attractive features of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks. These networks will consist of hundreds or thousands of self-organizing, low-power, low cost wireless nodes deployed en masse to monitor and affect the environment. Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real world challenges [4]. WSNs form an ad-hoc network that operate with nominal or no infrastructure. WSNs merge a wide range of information technology that spans multiple computer hardware vendors, software, networking and programming methodologies. WSNs make it possible to perceive what takes place in the physical world in ways, was not previously possible [5].

II. CHARACTERISTICS OF WSN

The main characteristics of a WSN include: WSN are getting a lot of popularity day by day due to their low costing solutions to variety of real world applications, many other favoring factors of WSN use are low power consumption constraints for nodes: portability, unattended operation, using batteries or energy harvesting, ability to with stand bad environmental conditions, having dynamic network topology, to cope with node malfunctioning and failures, Mobility of deployed nodes, Heterogeneity of nodes, Scalability, at the time of deployment and after deployment, Easy use.

III. SECURITY THREATS AND ISSUES IN WIRELESS SENSOR NETWORKS

Wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks. These issues are well-enumerated in some past researches [6] [7] [8] and also a number of security schemes are already been proposed to fight against them. The architectural aspect of wireless sensor network could make the employment of a security schemes little bit easier as the base stations or the centralized entities could be used extensively in this case.

Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks.

Sybil Attack

The sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack [9]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [10].

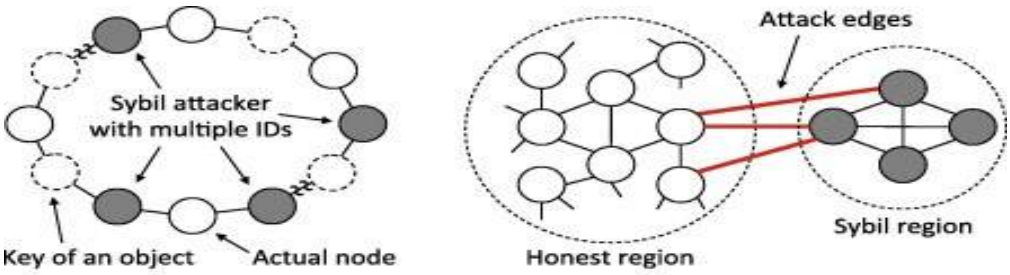

Figure 2: Sybil attack

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Black hole Attack

In this attack, a malicious node acts as a black hole [11] to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations.

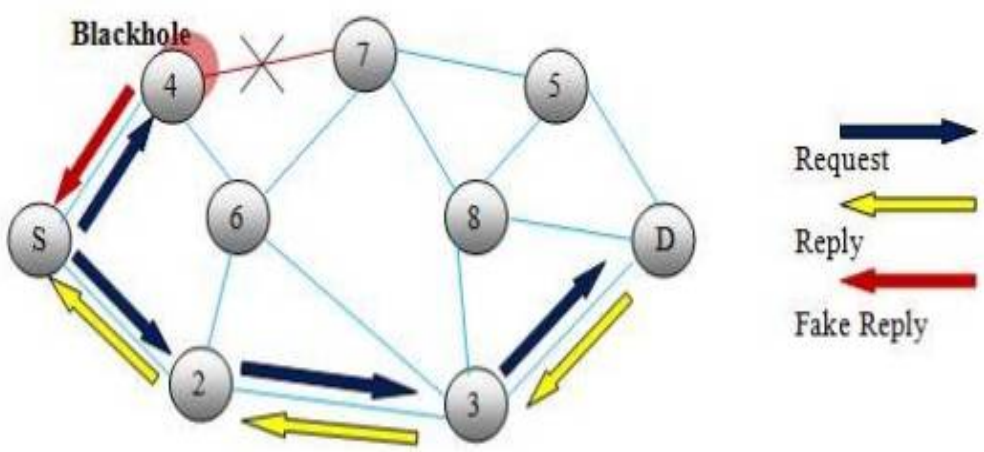

Figure 3: Black hole Attack

Wormhole attack:

In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. An attacker intrudes communications originated by the sender, copies a portion or a whole packet, and speeds up sending the copied packet through a specific *wormhole tunnel* in such a way that the copied packet arrives at the destination before the original packet which traverses through the usual routes.

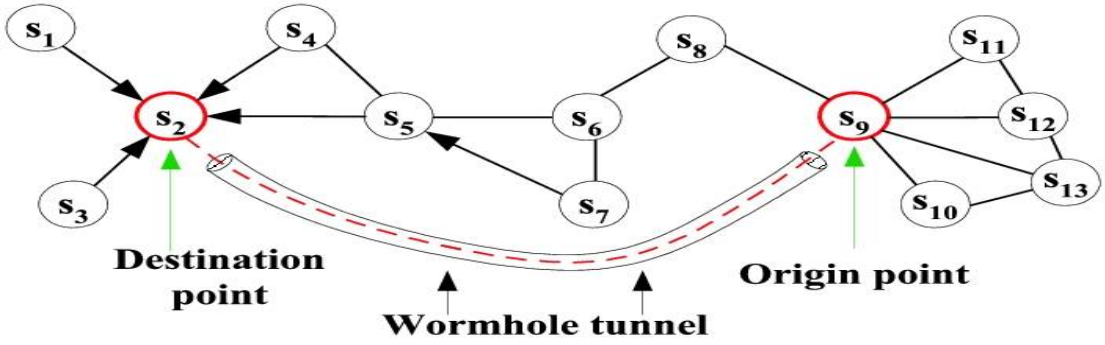

Figure 4: Wormhole Attack

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Spoofing Attack

In spoofing attack attacker complicates the network by creating routing loop, attracting or replaying the routing information.

Hello Flood Attack

Hello Flood Attack is introduced in [12]. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

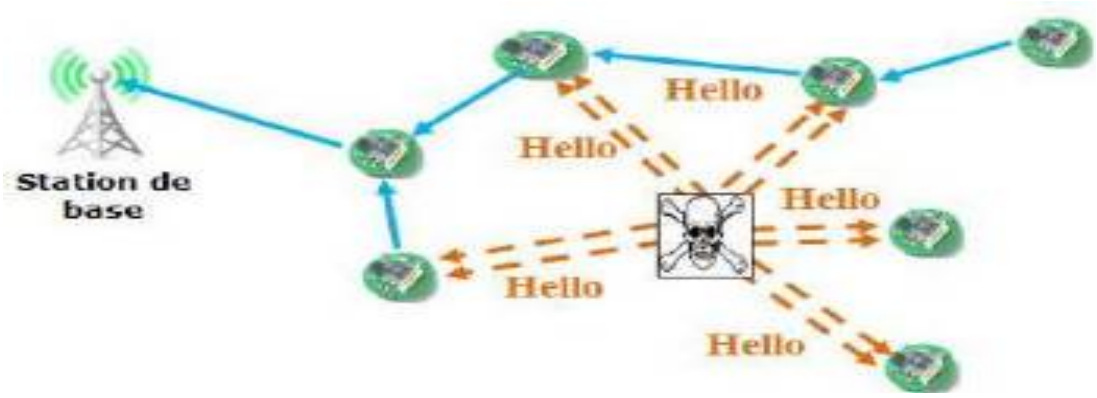

Figure 5: Hello Flood Attack

Sinkhole attack

The sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack, a compromised node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes with respect to the routing metric.

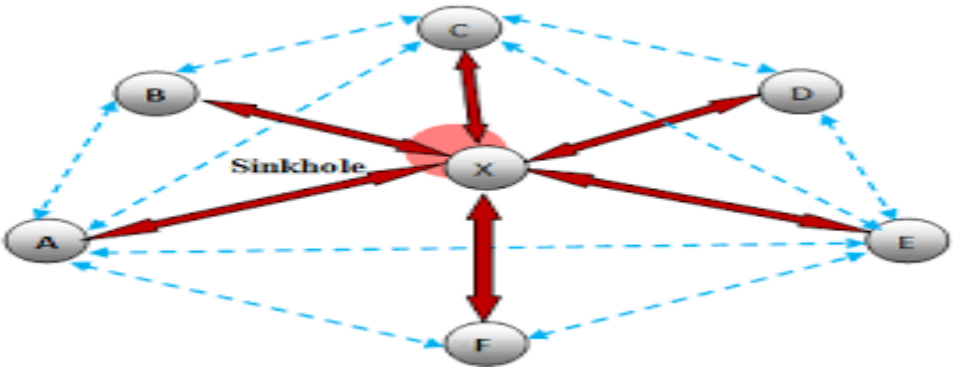

Figure 6: Sinkhole attack

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

IV. CHALLENGES OF SENSOR NETWORKS

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. A wireless sensor network is a special network which has many constraint compared to a traditional computer network.

Wireless Medium

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary.

The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks. [13]

Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration. Security schemes must be able to operate within this dynamic environment.

Hostile Environment

The next challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or capture by attackers. Since nodes may be in a
hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. cryptographic keys). The highly hostile environment represents a serious challenge for security researchers.

Resource Scarcity

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient. [14].

Immense Scale

The proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

V. CONCLUSION

Wireless sensor networks become more popular these days because of its low cost, less power requirement, performance and high potential application areas. This paper summarizes the security attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed. This survey will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

REFERENCES

1. Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
2. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E.,"Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.
3. Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.
4. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114, August 2002.
5. Satvika Khanna, Ms. Priyanka Singh, Akhil Kaushik "Wireless Sensor Network: Issues & Challenges" IJMA Vol 2, No 11, 2011
6. Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30.
7. Strulo, B., Farr, J., and Smith, A., "Securing Mobile Ad hoc Networks A Motivational Approach", BT Technology Journal, Volume 21, Issue 3, 2003, pp. 81 – 89.
8. Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, Volume 11, Issue 1, February 2004, pp. 38 – 47.
9. Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).
10. Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.
11. Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.
12. Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.
13. Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009
14. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006