WSN: Various Attacks & IDS in WSN

Amol N. Rindhe[1], **Sanjay V.Dhopte**[2]

[1]ME (IT) Scholar, PRMIT&R, Badnera
Sant Gadge Baba Amaravati Univercity, Amaravati, Chikhali - 443201 Maharashtra, India

[2]Proffessor (IT) PRMIT&R, Badnera
Sant Gadge Baba Amaravati Univercity, Amaravati, Amaravati-444601, India

Abstract: ***Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. Intrusion detection system in wireless sensor network is one of the growing research areas in recent years. Wireless sensor networks (WSN) consist of tiny devices. These tiny devices have limited energy, computational power, transmission range and memory. However, wireless sensor networks are deployed mostly in open and unguarded environment. Therefore, intrusion detection is one of the important aspects for wireless sensor networks. For the intrusion detection it is necessary to know the various attacks on WSN. In this report I mention several attacks on WSN and primarily focus only on the anomaly based intrusion detection system.***

Keywords: IDS, WSN, Anomaly, Security, Threats, Sensor Network

1. Introduction

Wireless sensor network is a collection of spatially deployed wireless sensors by which to monitor various changes of environmental conditions (e.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support [1]. Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Wireless sensor networks consist of some cheap and small devices. As they are generally deployed in unprotected environment, wireless sensor network is vulnerable to various attacks. Therefore, security design is one of the important factors for wireless sensor networks. There are two main techniques for security solution: prevention based and detection based. Prevention based techniques are encryption, authentication etc. Prevention based techniques cannot be applied to the wireless sensor networks because of the limited resources and broadcast medium. Detection technique is to identify the attacks based on the systems behavior. Currently, there are two different kinds detection technique: anomaly based and signature based.

2. WSN

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations [2]. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including n environment and habitat monitoring, healthcare applications, home automation, and traffic control. A Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors by which to monitor various changes of environmental conditions (e.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support .Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Due to a wide diversity of WSN application requirements, however, a general-purpose WSN design cannot fulfill the needs of all applications. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications [2].

3. Various Attacks on WSN

Wireless sensor network is vulnerable to several security threats. There are many papers [12] [4] [5] [6] [7] that provides the security threats in details. Here summarized some of the major security threats for WSN. Following Table summarizes all the security threats [13] [14].

a. Misdirection

Changing or replaying the routing information can cause the misdirection attack. Forwarding the message along with the wrong path can cause this kind of attack. Misdirection attack is also counted as routing layer attack.

b. Selective Forwarding

In this type of attack, attacker refuses to forward packets or drop them and act as a black hole.

c. Sinkhole Attack

In Sinkhole attack, attackers attract all the traffic from a particular area to a compromise node. This kind of attack can also cause selective forwarding attack.

d. Sybil Attack

In Sybil attack, a malicious node can represent multiple identities to the network.

e. Wormhole Attack

The simplest form of this attack is an attacker sits in between the two nodes and forward in between them.

f. Hello Flood Attack

In Hello Flood Attack, Attacker broadcast hello packets to the networks to add himself as the neighbor to the other nodes [14].

4. Intrusion Detection System (IDS) in WSN

Our intrusion detection model includes a network model, a detection model, and an intrusion strategy model. The network model specifies the WSN environment. The detection model defines how the intruder can be detected and the intrusion strategy illustrates the moving policy of the intruder.

4.1 Network Model

All sensors are static once the WSN has been deployed. In particular, we consider two WSN types: homogeneous and heterogeneous WSNs. In a homogeneous WSN, each sensor has the same sensing radius of r_s, and the transmission range of r_x.[3]

4.2 Detection Model

There are the detection models to recognize an intruder: single sensing detection model and multiple-sensing detection model. It is said that the intruder is detected under the single-sensing detection model if the intruder can be identified by using the sensing knowledge from one single sensor. On the contrary, in the multiple-sensing detection model, the intruder can only be identified by using cooperative knowledge from at least k sensors (k is defined by specific application requirements).

In order to evaluate the quality of intrusion detection in WSNs, we define three metrics as[15]:

1. **Intrusion distance.** The intrusion distance, denoted by D, is the distance that the intruder travels before it is detected by a WSN for the first time. Specifically, it is the distance between the point where the intruder enters the WSN and the point where the intruder gets detected by any sensor(s). Following the definition of intrusion distance, the Maximal Intrusion Distance is the maximal distance allowable for the intruder to move before it is detected by the WSN.
2. **Detection probability.** The detection probability is defined as the probability that an intruder is detected within a certain intrusion distance (e.g., Maximal Intrusion Distance).
3. **Average intrusion distance**. The average intrusion distance is defined as the expected distance that the intruder travels before it is detected by the WSN for the first time.

4.3 Intrusion Strategy Model

We consider two intrusion strategies for the movement of the intruder in a WSN. If the intruder (say, a panzer) already knows its destination before entering the network domain, it follows the shortest path to approach the destination. In this case, the intrusion path is a straight line from the entering point to the destination. The main idea behind this strategy is that the straight movement causes the least risk for the intruder due to the least area that it has to explore by following a straight line toward the destination. The corresponding intrusion detection area S1 is determined by the sensor's sensing range rs and intrusion distance D1. It is because the intruder can be detected within the intrusion distance D1 by any sensor(s) situated within the area of S1 [15].

5. Conclusion

Wireless sensor networks are vulnerable to several attacks because of their deployment in an open and unprotected environment. In this I describe the major security threats in WSN and also describe different intrusion detection techniques and also describe several existing approaches to find out how they have implemented their intrusion detection system. This paper analyzes the intrusion detection problem in both homogeneous and heterogeneous WSNs.

6. References

[1] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu, and T.L. Porta,"Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 6, June 2007

[2] G.Li, J. He, Y. Fu. "Group-based intrusion detection system in wireless sensor networks" Computer Communications, Volume 31 , Issue 18 (December 2008)

[3] Krontiris, I., Dimitriou, T., Freiling, F.C.: Towards intrusion detection in wireless sensor networks. In: Proceedings of the 13th European Wireless Conference, Paris, France (April 2007)

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications Anchorage, AK, May 11, 2003).

[5] D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks", Computer, v.35 n.10, p.54-62, October 2002

[6] Perrig, J. Stankovic, and D.Wagners, "Security in wireless sensor networks", Communications of the ACM, Volume 47, Issue 6 (June 2004).

[7] A.S.K. Pathan, H-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges", Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, Vol.2, Iss., 20-22 Feb. 2006

[8] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM Wireless Networks, vol. 9, no. 5, Sept. 2003, pp. 545–56

[9] V. Bhuse, A. Gupta, "Anomaly intrusion detection in wireless sensor network" Journal of High Speed Networks, Volume 15, Issue 1, pp 33-51, Jan 2006

[10] An intrusion detection system for wireless sensor networksOnat, I.; Miri, A. Wireless And Mobile

Computing, Networking And Communications, 2005. (WiMobapos;2005), IEEE International Conference on Volume 3, Issue , 22-24 Aug. 2005

[11] da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized intrusion detection in wireless sensor networks", Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks- 2005.

[12] R. Roman, J. Zhou, and J. Lopez, "On the Security of Wireless Sensor Networks", Proceedings of 2005 ICCSA Workshop on Internet Communications Security, pp 681-690, LNCS 3482, Singapur, May 2005.

[13] F. Akyildiz*et al.*, "Wireless Sensor Networks: A Survey," Elsevier Comp. Networks, vol. 3, no. 2, 2002,pp. 393–422.

[14] Md.Safiqul Islam,Syed Ashiqur Rahman "Anomaly Intrusion Detection System in WSN: Security threats and existing approaches",Nov-2011.

[15] X. Wang, Y. Yoo, Y. Wang, and D.P. Agrawal, "*Impact of Node Density and Sensing Range on Intrusion Detection in Wireless Sensor Networks,"* Proc. 15th Int'l Conf. Computer Comm. and Networks (ICCCN '06), Oct. 2006.

[16] D.P. Agrawal and Q.-A. Zeng, Introduction to Wireless and Mobile Systems. Brooks/Cole Publishing, Aug. 2003.

[17] Liu and D. Towsley, "Coverage of Sensor Networks: Fundamental Limits," Proc. Third IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS), Oct. 2004.

Author Profile

Mr. Amol N. Rindhe is student of second year M.E. (Information Technology) PRMIT&R, Badnera, Amravati – Sant Gadge Baba Amravati University, Amravati, India

Mr. Sanjay V. Dhopte is Professor (Information Technology) PRMIT & R, Badnera, Amravati- Sant Gadge Baba Amravati University, Amravati, India.