Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches

Md. Safiqul Islam [*1], Syed AshiqurRahman[*2]

Department of Computer Science and Engineering
Daffodil International University, Dhaka, Bangladesh

1. safiqul@daffodilvarsity.edu.bd, 2. ashiq797@daffodilvarsity.edu.bd

Abstract

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. There are two different kind of intrusion detection mechanism: anomaly based and signature based. In this paper, we mention several attacks on WSN and we primarily focus only on the anomaly based intrusion detection system. Finally, we discuss about several existing approaches to describe how they have identified security threats and implemented their intrusion detection system.

Keywords: *WSN, IDS, Sensor Networks, Anomaly, Security, Threat.*

1. Introduction

Wireless ad hoc networks (WAHN) are autonomous nodes that communicate with each other in a decentralized manner through multi-hop routing. There are two main types of WAHNs, namely: mobile ad hoc networks (MANET) and wireless sensor networks (WSN). Varieties of potential applications such as environment monitoring, health monitoring, military solution are provided by WSN [1]. 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. In this paper we will focus only towards the anomaly based detection technique. Most of the WSN researches were based on homogeneous and heterogeneous network [2]. In homogeneous networks, all the sensor nodes have the same capability; on the other hand, sensor nodes may be of varying capabilities in heterogeneous networks. In this paper, we have focused on the various threats on WSN and then we focused on some existing approaches to find out how they have implemented their intrusion detection system (IDS) for wireless sensor networks.

2. Characteristics of Wireless Sensor Networks

2.1 Self-Organization

Wireless sensor networks are formed by deploying large number of sensor nodes in a region. Sensor networks protocols and algorithms have self-organizing capability.

2.2 Multi hop Routing

Because of the short transmission range, sensor nodes use multi-hop routing to forward their data to the upper nodes.

2.3 Resource Limitation

Wireless sensor nodes have limited battery life, shorter transmission range and computational power. They also have limited memory.

3. Comparison with MANET

IDS proposed in ad hoc network cannot be implemented directly in the sensor networks because of the following reasons:

- Number of nodes in WSN is higher than the node in ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failure.
- Dynamic topology in WSN.
- Broadcast medium used by WSN.
- Limited resources in WSN.

4. Various Attacks on WSN

Wireless sensor network is vulnerable to several security threats. There are many papers [3][4][5][6][7] that provides the security threats in details. Here we have summarized some of the major security threats for WSN. Table 1 summarizes all the security threats.

4.1 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.

4.2 Selective Forwarding

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

4.3 Sinkhole Attack

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

4.4 Sybil Attack

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

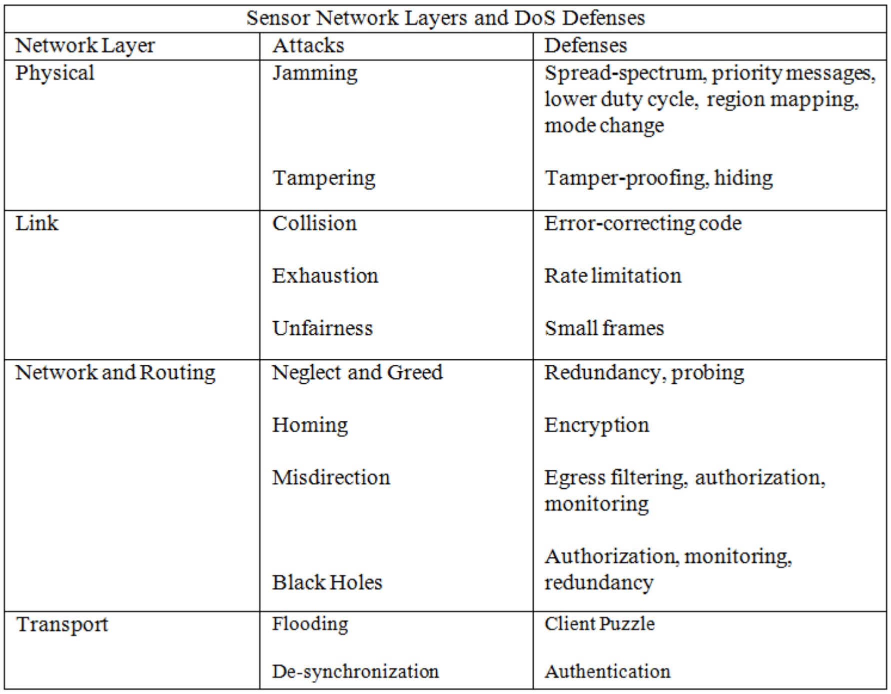
4.5 Wormhole Attack

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

4.6 Hello Flood Attack

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

Table 1. Different DoS attacks and Defense Mechanisms in WSN[7]



Sensor Network Layers and DoS Defenses		
Network Layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network and Routing	Neglect and Greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black Holes	Authorization, monitoring, redundancy
Transport	Flooding	Client Puzzle
	De-synchronization	Authentication

5. Intrusion Detection System

Intrusion detection is a set of actions that determine, and report unauthorized activities. It detects the violation of confidentiality, integrity and availability. There are two types of detection technique: signature detection and anomaly detection [8]. IDS with signature detection based compares the current activity of the nodes with the stored attack profiles and generate an alarm based on the profile. On the other hand, anomaly based compares the systems normal profile with the current activity. In this paper, wehavedescribed several existing approaches based on anomaly intrusion detection technique.

5.1 Anomaly Intrusion Detection based on OSI Layer

In [9] there is description of intrusion detection based on anomaly in multiple layers. The paper tried to detect intrusion based on multiple OSI layers to reduce the false alarm rates.

5.1.1 Physical Layer: Received Signal Strength Indicator (RSSI) value is used at the physical layer. During the neighbor discovery, each node records the RSSI value received from its neighbor. Therefore, any node receiving packet with unexpected RSSI value will generate an alarm. However, there is a chance of high positive false alarm because RSSI value is affected with the background noise.

5.1.2 Mac Layer: At Mac layer, the authors proposed to use time scheduling algorithm such as TDMA to allocate the time slot to each node and SMAC to allocate wake and sleep schedule. If node A received packets from node B at the time when B is supposed to sleep then alarm will be raised.

5.1.3 Routing Layer: At the routing layer, they have used forwarding tables generated by the routing protocol. And they have also proposed a protocol named *information authentication for sensor network* (IASN). The protocol works on authenticating information rather than authenticating nodes. That means, a node keeps track on its neighbors and knows what kind of information it expects from its neighbors. As an example, if a node receives a packet from node B but it is expecting the packet from node C then an anomaly is detected. In the paper, they have also shown how IASN works with routing protocols like DSR, DSDV and directed diffusion.

5.1.4 Application Layer: At application layer, they have proposed mutual guarding techniques. In the mutual guarding technique, the author described about nodes guarding each other and also mentioned about four nodes guarding each other.

5.2 Anomaly Intrusion Detection based on Sliding Window

In [10], the authors have introduced an intrusion detection algorithm to consider the node impersonation attack and route depletion attack. Their detection algorithm is based on the sliding window approach where N packets are buffered. If the comparison of the rate of the N received packets and rate of the previous N received packet is greater than a threshold value then the alarm is triggered. But the algorithm fails to mitigate all the security threats.

5.3 Anomaly Intrusion Detection based on rules

In [11], the authors have proposed several rules to detect anomaly. The rules are:

- **Interval Rule:** A failure is detected if two consecutive message receptions are smaller or greater than the allocated time.
- **Retransmission Rule:** A failure is detected if the node is not forwarding the message. This rule can detect black hole and selective forwarding attack.
- **Integrity Rule:** A failure is raised if an attacker modifies the message payload.
- **Delay Rule:**A failure is detected if the message is not delivered on due time.

- **Repetition Rule:** This rule detects denial of service attack where a failure is detected if the same message is sent by node several times than expected.
- **Radio Transmission Range:** A failure is raised if the message is received from the other node except from one of its neighbor. All the message listened by monitor node must be originated by one its neighbor.
- **Jamming Rule:** The number of collisions associated with a message must be lower than the expected number of collisions.

They have implemented IDS in some of the nodes called monitor node and their monitor nodes functionalities are shown in figure 1.

Monitor node will act as an ordinary node and also it will detect intrusion in three phases. Phase 1 will collect data and send it to the phase 2 to check the data by predefined rules and then intrusion alarm is raised at phase 3.

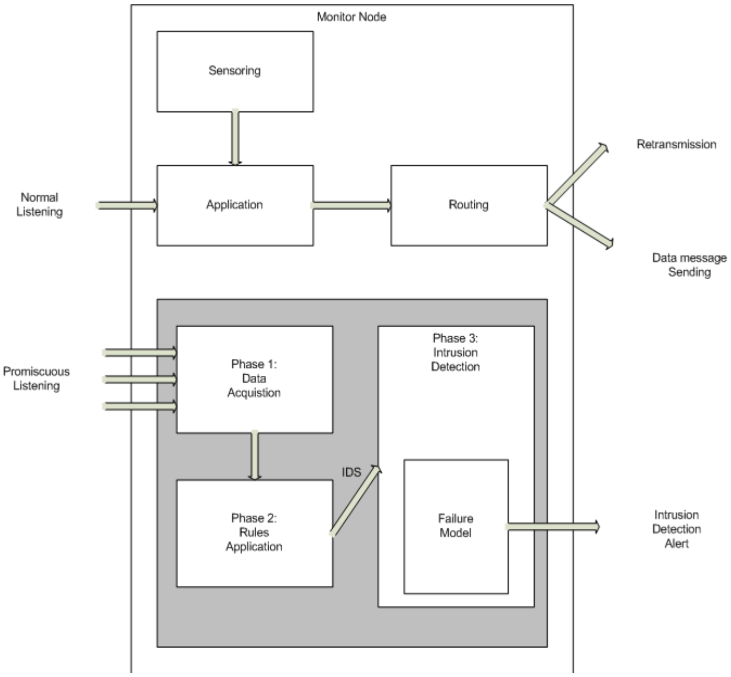


Figure 1. Monitor Node Adapted from [11]

5.4 Anomaly Intrusion Detection based on Delta Grouping Algorithm

Li, He and Fu in [12] proposed a group based IDS which is based on anomaly detection technique. They have used delta grouping algorithm to partition the network into groups and then run the detection algorithm on each groups. At first, the whole sensor nodes are deployed in the network and then the delta algorithm is applied to partition the network and then IDS is applied on each group.

5.5Anomaly Intrusion Detection for Black Hole Attack

In [13], the authors have proposed their own IDS algorithm to detect black hole and selective forwarding attack and they have proposed two rules to detect anomaly:

Rule 1: If the node A send a packet to node B than it stores the packet in its buffer and watch whether B forwards it or not. If B doesn't then increment then counter by one or delete the message. If the failure count is more than the threshold value, an alarm will be raised.

Rule 2: If the majority of the monitor nodes have raised an alert then the target node is compromised and should be revoked or should be notified by the base station. Based on their rules, they have proposed an IDS block that is implemented in all the sensor nodes.
Figure 2 illustrates how IDS agent works in each sensor node:

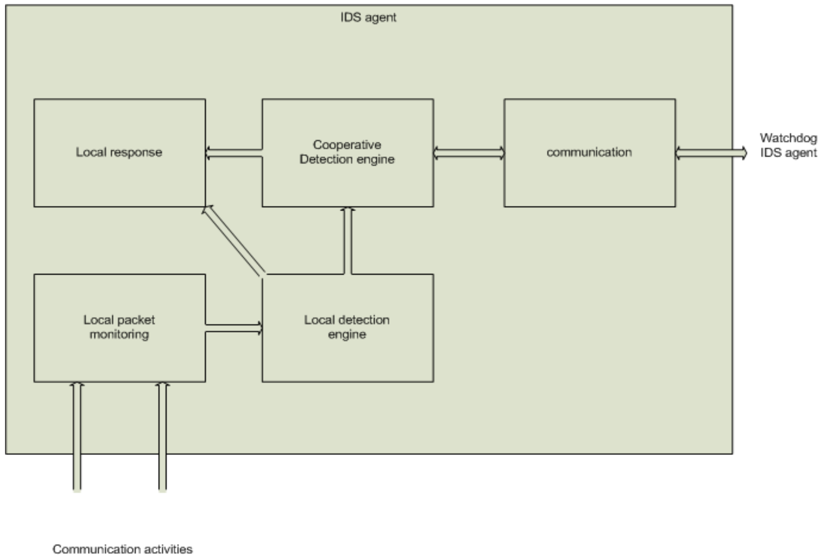


Figure 2. IDS Building Agent, taken from [13]

They proposed an IDS agent in each sensor node and their IDS agent consists of following

- Local responses
- Cooperative detection engine.
- Communication
- Local packet monitoring
- Local detection engine

Local responses send the response to the base station if any anomaly is found. In cooperative detection engine phase, if any of the node detects the intrusion then it shares information with the other nodes to reduce the false alarm rates. However, the local packet monitoring phase monitors the packet and sends the data to the detection engine phase to detect the intrusion to detect the anomaly based on their unexpected behavior,

6. Conclusion

Wireless sensor networks are vulnerable to several attacks because of their deployment in an open and unprotected environment. This paper describes the major security threats in WSN and also describes different intrusion detection techniques. Moreover, the paper also describes several existing approaches to find out how they have implemented their intrusion detection system.

References

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

[2] 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

[3] 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.

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

[6] A. Perrig, J. Stankovic, and D.Wagner, "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] A. 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] G.Li, J. He, Y. Fu. "Group-based intrusion detection system in wireless sensor networks" Computer Communications, Volume 31 , Issue 18 (December 2008)

[13] 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)

Authors

Md. Safiqul Islam is currently working as a Lecturer in Daffodil International University. He has completed his M.Sc. in Internetworking from Royal Institute of Technology, Sweden and completed his B.Sc. in Computer Engineering from American International University in Bangladesh. He has done his Master's thesis in Ericsson Research, Sweden where he has implemented and evaluated a HTTP Streaming Video Server that supports dynamic advertisement splicing. He has also worked as a project coach at Telecommunication System Lab at KTH where he was responsible for coaching R&D projects. Besides that, he has also worked as a Software Quality Assurance Engineer and Network. Operation Center Engineer in two renowned companies in Bangladesh. His research interests lies in next generation computer networks, video streaming in internet, peer to peer network, wireless sensor networks and mobile networks.

Syed Ashiqur Rahman is currently teaching as a lecturer (CSE) in Daffodil International University. He has completed his B.Sc. in Computer Science and Engineering from University of Dhaka in Bangladesh. He joined as a member of Network & Technology Consultant (N&TC) department in Ericsson Bangladesh Ltd. Besides that, he has also worked as a Software Programmer in a software company. His research interests lies in wireless sensor networks, mobile ad-hoc networks, networks security & cryptography, peer to peer network, algorithms.