A Hierarchical Intrusion Detection System in Wireless Sensor Networks

Md. Safiqul Islam[†] **Razib Hayat Khan**[††] **Dewan Muhammad Bappy**[†††]

[†] School of Information and Communication Technology,
Royal Institute of Technology (KTH), Stockholm, Sweden

[††]Department of Telematics,
Norwegian University of Science and Technology (NTNU), Trondheim, Norway

[†††]Department of Electrical Engineering,
Blekinge Institute of Technology, Karlskrona, Sweden

Summary

Wireless sensor networks (WSNs) often consist of tiny devices with limited energy, computational power, transmission range, and memory. WSNs offer a variety of potential means to monitor environments. However, WSNs are vulnerable to various attacks because these networks are often deployed in open and unprotected environments. Therefore, security design is an important aspect of WSNs. In this paper, we describe various threats to WSN and then examine existing approaches to identify these threats. Finally, we propose an intrusion detection mechanism based on these existing approaches to identifying threats.

Keywords:
WSN, IDS, Sensor networks.

1. Introduction

Wireless sensor networks (WSNs) have emerged as one of the hottest research areas in recent years. Numerous potential economically viable applications include environment monitoring, health monitoring, and military applications [1]. WSNs typically consist of small inexpensive devices deployed in open, unprotected, and unattended environments for long term operations to monitor and collect data. This data is subsequently reported back to a base station over a wireless link. A WSN is vulnerable to various attacks; hence security is an important factor in the design of WSNs. However, sensor nodes have limited memory, power, computational capability, and transmission range [1], so security needs to be implemented keeping in mind these limited resources.

In general, security solutions for WSNs can be categorized into two main techniques: prevention based and detection based. Prevention techniques such as encryption and authentication are tricky for WSNs because of the limited resources and the use of a broadcast medium. Detection techniques identify the attacks based on the system's behavior. WSNs can be categorized into two types based on the nodes' capabilities [2]: a homogeneous network where every sensor node has same capability and a heterogeneous network where some of the nodes have greater capabilities (such as longer transmission range).

This paper describes the security threats and various kinds of attacks on WSNs and describes the need for an intrusion detection system (IDS) in WSNs. We mention some existing approaches to implement IDS for a WSN. The remainder of the paper is organized as follows. Section 2 gives an overview of the challenges and security threats for WSNs, and requirements for an application on WSN. Several intrusion detection techniques are introduced in section 3. In section 4, we describe several existing approaches. In section 5, a proposal for IDS in wireless sensor network is introduced based on the existing approaches. Finally, section 6 gives our conclusion.

2. WSN Security Threats

WSNs are vulnerable to several security threats. There are many papers [4][5][6][7][8] that describe these security threats. In this section, we will summarize all of these security threats and challenges. We follow Edith Nagai's classification of these attacks into different layers [9].

Manuscript received August 5, 2010
Manuscript revised August 20, 2010

2.1 Physical Attack

Physical access to the sensor node is possible because of the placement of sensor nodes in an unguarded environment. Therefore an intruder may be able to damage or tamper with the sensor devices.

2.2 Link Layer Attack

Jamming, collisions, or corruption at the link layer can delay the packet transmission or cause the packet to be lost or corrupted.

2.3 Network Layer Attack

Most attacks in WSN target the routing layer. Some network layer attacks are described in table 1. For further details see [5].

Table 1: Network Layer Attacks

Misdirection	Misdirection is based upon changing, spoofing, or replaying the routing information. By forwarding the message along with the wrong path or by sending false routing updates can lead to this kind of attack.
Selective Forwarding	In this kind of attack, attacker may refuse to forward packets or drop them and act as a black hole. Also, it can forward to packet to wrong receiver.
Sinkhole Attack	In a Sinkhole attack [10], Attacker‘s goal is to lure all the traffic from a particular area to a compromise node. This attack may create also selective forwarding attack.
Sybil Attack	In a Sybil attack [11], a malicious node can represent multiple identities to the network. This kind of attack is threatening to fault tolerant schemes such as distributed storage , multipath routing and topology maintenance
Wormhole Attack	In a wormhole attack [12], an adversary receives message from one part of network and tunneled message to the other part of the network. The simplest form of this attack is an attacker sits in between the two nodes and forwards packets between them.
Hello Flood Attack	In a Hello Flood Attack, the attacker broadcasts hello packets to convince the nodes that the attacker is a neighbor.

2.4 Application Layer Attack

The most common application layer attack is a denial of service (DOS) attack [6]. A DOS attack interrupts the network’s ability to perform its expected function. A DOS attack can be caused by hardware failures, software bugs, resource exhaustion, and environmental conditions.

3. Intrusion Detection System

Intrusion detection is a set of actions that discover, analyze, and report unauthorized and damaging activities. The goal is to detect violations of confidentiality & integrity, and reduced availability of resources. An IDS monitors the network and improves the user’s activity to detect intrusion.

Generally, there are two major types of detection techniques: signature detection and anomaly detection [13]. Signature detection is based on creating a profile of known attack signatures, then an IDS implements signature detection by comparing current activity with each of the stored attack profiles. The system generates an alarm if a match is found. Unfortunately, signature based detection will fail to detect new types of attack. In contrast, anomaly detection creates normal profiles of system behavior. It compares the system’s normal profile(s) with the current activity. The main drawback of anomaly based technique is that it generates of lots of false alarms [14].

A new approach is specification based technique. This alternative combines the advantages of both signature based and anomaly based intrusion detection system by using manually developed specifications to describe the normal system behavior, thus, reducing the rate of false alarms.

In [15], Y. Wang divides intrusion detection techniques into single-sensing detection and multi-sensing detection. In single-sensing detection, the intruder can be successfully detected by one sensor. While in multi-sensing detection, multiple collaborating sensors are used to detect the intrusion.

4. Existing Approaches

Several intrusion detection techniques have been proposed for use in *ad hoc* networks. However, many of these IDS solutions (such as those in [5][13][16][17]) cannot be implemented in sensor networks because of the limited resources in the sensor nodes. In this section, we will describe some existing proposals for intrusion detection in WSNs.

4.1 Anomaly Intrusion Detection

V. Bhuse and A. Gupta in [18] describe a system for intrusion detection based on anomaly intrusion detection techniques in multiple layers detection system more robust. In their approach, they try to detect intrusion based on physical, link, network, and application layers. At the physical layer, the Received Signal Strength Indicator (RSSI) value is used to detect anomalies. During neighbor discovery, each node records the RSSI value received from its neighbor. Therefore, any node receiving a packet with an unexpected RSSI value will generate an alarm. However, this has a high positive false alarm rate because the RSSI value is affected by the background noise. At the link layer, if a time scheduling algorithm is used to allocate time slots to each node, and then if node A receives packets from node B when B is supposed to be sleep an alarm will be raised.

At the network layer, they propose a protocol named *information authentication for sensor network* (IASN). This protocol works by authenticating information, rather than authenticating nodes. Thus a node keeps track of its neighbors and knows what kind of information it expects from its neighbors. Then if a node receives a packet from node B, but it is only expecting such a packet from node C - then an anomaly is detected. They showed IASN works with routing protocols such as DSR [19], DSDV [20], and directed diffusion.

At the application layer, they proposed mutual guarding techniques and use of round trip times. Unfortunately, round trip times have very high false positive rates because of background noise, weather, etc. In the mutual guarding technique, the authors described how nodes guard each other and give an example of four nodes guarding each other. If an intruder tries to attack from the mutual area of these four nodes, then other three nodes will detect an anomaly. Their paper does not describe how the sensor nodes will be organized in the network.

Onat and Miri introduced an intrusion detection algorithm to address a node impersonation attack and route depletion attack [21]. Their detection algorithm is based on a sliding window approach where N packets are buffered. If the rate of the most recent N received packets and rate of the previous N received packet are greater than a threshold, then an alarm is triggered. However, this algorithm fails to mitigate all the security threats.

4.2 Decentralized Intrusion Detection

Da Silva, et al. propose an intrusion detection algorithm that is divided into three phases [22]. Phase 1 is a data acquisition phase. During this phase a monitor node listens in promiscuous mode and stores the required information utilizing the memory of the sensor node. The authors define a set of rules (shown in table 2) that are applied in phase 2 to the stored data. If the message fails any of the rules, then a failure counter is increased. Finally, Phase 3 compares the failure count with the threshold value. If the number of failure is greater than a threshold, then an alarm will be raised.

Table 2: IDS Rules

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 in due time.
Repetition Rule	This rule detects denial of service attack where a failure is detected if the same message is sent by node more times than expected.
Radio Transmission Range	A failure is raised if the message is received from a node other than one of its neighbors. All the message received by a 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.

4.3 Distributed approach for detecting black hole and selective forwarding

Krontiris, Tassos, and Felix in [23], proposed an IDS in each sensor node with two rules for detecting a black hole and selective forwarding attack. They propose that if a node is sending messages, then its entire neighbor will monitor this node. The first rule is, if the node A sends a packet to node B, then the monitoring node stores the packet in its buffer and watches to see whether B forwards it or not. If B does not forward the packet, then a counter is incremented by one. When the failure count exceeds a threshold value, then an alarm will be raised. The second rule is: if the majority of the monitor nodes have raised an alert, then the target node is compromised.

4.4 Spontaneous watchdog

Roman, Zhou, and Lopez proposed a novel technique to monitor neighbors named “spontaneous watchdog” [24]. They utilize (1) a local agent that monitors local activities and the information exchanged each sensor and (2) a global agent that monitors the communication between neighbors.

Their spontaneous watchdog technique relies on the broadcast nature of sensor networks. Their global agent works as a spontaneous watchdog. Initially, all active nodes will receive the packets because of the broadcast nature of the transmission. When a node receives a packet, then it will check if it is the destination of the packet. If it is not, then it will not drop the packet. The node will also check whether the receiver is in its neighborhood. If so, then this node will act as a spontaneous watchdog and will verify how many nodes activated themselves as spontaneous watchdog.

4.5 Other Existing Approaches

Y. Wang, et al. [15], propose an analytical model for intrusion detection. They use this model for single-sensing detection and multiple-sensing detection in both homogeneous and heterogeneous networks. Their paper also deals with network connectivity and broadcast reach ability.

Li, He and Fu [25] propose a group based intrusion detection system based on anomaly detection. They use a delta grouping algorithm [26] to partition the network into groups, then run their detection algorithm on each group.

Agah, et al. propose a non-cooperative game theory approach to detect the most vulnerable node in the network [27].

5. Our Proposed Model

In this section, we propose an intrusion detection system for wireless sensor network. Our intrusion detection system is a four layer architecture and uses the specification based detection technique. The following subsections describe our architecture and techniques in more detail.

5.1 Network Architecture

Our network architecture is based on four layers. The bottom layer consists of all leaf level sensors that collect data from the environment. The second and third layers consist of monitor nodes; where the second layer monitors the communication pattern of leaf level sensors. Level 3 sensors monitor the behavior of level 2 sensors. The placement of level 3 sensors should be such that each can monitor the communication of two level 2 sensors. Finally, the top layer is the base station, usually operated by a human. Figure 1 illustrates how the sensor nodes are organized into a network. This approach requires a heterogeneous network with level 2 and level 3 sensors being more powerful than the leaves in terms of both transmission range and battery life.

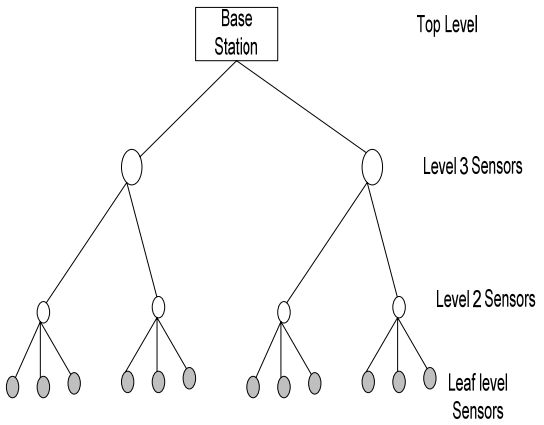

Figure 1: Network Architecture

All the leaf level sensors deployed in the network are divided into several groups. This network partition can be done using the delta grouping algorithm [25]. For each group we deploy one level 2 sensor to monitor the group. Level 2 and level 3 sensors implement the IDS solution. Each leaf level sensor sends data to a level 2 sensor. The level 2 sensor aggregates all the data and sends it to a level 3 sensor. Level 3 sensors monitor the level 2 sensor's behavior. Each level 3 sensor must be placed within range of two level 2 sensors from where it can watch the communication of these two sensors. If an anomaly is detected by a level 2 sensor, it raises an alarm and sends it to level 3, where the alert is investigated and if it is valid, then an alarm with aggregated data is sent to the base station.

5.2 Intrusion Detection Technique

We have modified the intrusion detection algorithm proposed by Da Silva, et al. [22] and implemented in our level 2 and level 3 sensors. Due to their limited resources, we have not implemented any IDS in the leaf level sensors. Monitor nodes functionalities are divided into three phases. Phase 1 all the leaf level sensors collect information from their environments and report it to the level 2 sensors. In phase 2, rather than using the rules described in [22], we have used layer based attack detection in phase 2 to detect attacks as proposed in [18]. Table 4 describes how attacks are detected in several layers. This layered based attack detection makes our system more robust. Phase 3 compares each report to the defined the threshold value to decide whether it should raise an alarm. Phase 3 is used to reduce the false alarm rate. Threshold values can be defined manually or adjusted based on the requirements of a particular WSN. Thus, our proposed architecture can detect most of the security threats by reducing the false positive alarms.

Table 4: Layered based attack detection

Physical Layer	During the receiving information from leaf level sensors, level 2 sensors record the RSSI value. After that, It compares the stored RSSI value with received RSSI value to detect anomaly. Similarly, level 3 sensors record the RSSI value of level 2 sensors to detect the intrusion.
Link Layer	TDMA has been used to assign time slots for the leaf level sensor nodes. SMAC has been used to allocate wake and sleep schedule to save resources in the leaf level sensors and level 2 sensors. Thus, a level 2 or level 3 sensors can easily detect intrusion if it receives data from some sensors who are not allocated to use that time slot.
Network Layer	Use of IASN protocol proposed in [18], both level 2 and level 3 sensors can easily detect whether the packet has come from the correct source or not.
Application Layer	We have used our own three level monitoring techniques in the application layer instead of mutual guarding proposed in [18]. Three level monitoring techniques are: (1) Leaf level sensors are monitored by level 2 sensors, (2) Level 2 sensors are monitored by level 3 sensors, and (3) Level 3 sensors are monitored by base station.

6. Conclusions

In this paper, we have presented the security threats and challenges in WSNs. We investigated several existing intrusion detection approaches to learn how they have implemented their intrusion detection. We proposed a hierarchical intrusion detection system based on a synthesis of the existing approaches. Future work will focus on implementing our proposed architecture on a simulator.

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] D. Culler, D. Estrin, and M. Srivastava, "Sensor Networks: an Overview," *IEEE Computer Magazine*, August 2004

[4] 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.

[5] 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).

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

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

[8] 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

[9] E. C.H Nagai, "Intrusion Detection for Wireless Sensor Networks" Ph.D. Term 2 Paper, The Chinese University of Hong Kong. Department of Computer Science and Engineering. www.cse.cuhk.edu.hk/~lyu/student/phd /edith/edith_term2.pdf

[10] E.C.H., Ngai, J. Liu, and M.R. Lyu, On the intruder detection for sinkhole attack in wireless sensor networks. In: ICC 2006. Proceedings of the IEEE International Conference on Communications, Istanbul, Turkey (2006)

[11] J. Newsome, E. Shi, D. Song, and A. Perrig, "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

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002

[13] 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

[14] F. Cuppens and A. Miege:, Alert correlation in a cooperative intrusion detection framework. In: Proceedings of IEEE Symposium on Security and Privacy (2002)

[15] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal: Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks. IEEE Trans. Mobile Computing, 7(6): 698-711 (2008)

[16] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu. Adaptive Security for Multi-Layer Ad-Hoc Networks. Special Issue of Wireless Communications and Mobile Computing, 2002

[17] P. Albers, O. Camp, J. Percher, B. Jouga, L. Me, and R. Puttini. Security in ad hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches. 1st International Workshop on Wireless Information Systems (WIS'02), April 2002.

[18] 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

[19] D. Johnson and D. Maltz. "Dynamic source routing in ad hoc wireless networks," Mobile Computing (ed. T.

Imielinski and H. Korth), Kluwer Academic Publishers, Dordrecht, The Netherlands, 1996.

[20] C. Perkins and P. Bhagwat. "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", proceedings of the ACM SIGCOMM, October 1994.

[21] I. Onat and A. Miri, An intrusion detection system for wireless sensor networks. IEEE International Conference Wireless and Mobile Computing, Networking, and Communications, 2005. (WiMobapos;2005) , Volume 3, Issue , 22-24 Aug. 2005

[22] 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.

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

[24] R. Roman, J. Zhou, and J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks", Proceedings of 2005 ICCSA Workshop on Internet Communications Security, LNCS 3482, May 2005, pp 681-690

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

[26] A. Meka, A.K. Singh, Distributed Spatial Clustering in Sensor Networks, Lecture Notes in Computer Science 3896, Springer Verlag, Heidelberg, Germany, 2006, pp. 980-1000.

[27] Afrand Agah , Sajal K. Das , Kalyan Basu, and Mehran Asadi, Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach, Proceedings of the Third IEEE International Symposium on Network Computing and Applications, August 30-September 01, 2004, p.343-346.

Md. Safiqul Islam 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.

Razib Hayat Khan is doing his PhD at Department of Telematics, Norwegian University of Science and Technology (NTNU), Norway. He completed his M.Sc. in Information & Communication Systems Security specialized in Security in Open Distributed System from Royal Institute of Technology (KTH), Sweden in 2008. He worked under VRIEND project (http://vriend.ewi.utwente.nl) as part of his M.Sc. thesis which was sponsored by Sentinels, a joint initiative of the Dutch Ministry of Economic Affairs, the Netherlands organization for Scientific Research Governing Board and the Technology Foundation STW and the industrial partners were Philips Electronics, AkzoNobel, Corus, and DSM. He also worked as research engineer, Multimedia technologies at Ericsson AB, Sweden. He received his B.Sc. degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Gazipur, Bangladesh in 2004. He served as a lecturer in Stamford University, Dhaka, Bangladesh during the period November 2004 – August 2006. He received the OIC (Organization of the Islamic Conference) scholarship for three years during his BSc studies. His research interest is mainly focused on Network performance modeling, Information Systems Security. At present he is working with performance and security issues in Communication system.

D.M. Bappy has completed his B.Sc. from American International University Bangladesh (AIUB) in Electrical and Electronic Engineering in May, 2007. After that he started to work as a Lecturer in the department of Electrical and Electronic Engineering in the World University of Bangladesh from June, 2007 to July, 2008. Now he is studying M.Sc. in electrical engineering with emphasize on Signal Processing in Blekinge Institute of Technology. His research interests lies in the area of robotics, computer vision, image processing and signal processing.