Intrusion Detection Systems for Wireless Sensor Networks: A Survey

Ashfaq Hussain Farooqi and Farrukh Aslam Khan

FAST National University of Computer and Emerging Sciences,
A. K. Brohi Road, H-11/4, Islamabad, Pakistan
{ashfaq.farooqi,farrukh.aslam}@nu.edu.pk

Abstract. Wireless sensor networks (WSNs) are vulnerable to different types of security threats that can degrade the performance of the whole network; that might result in fatal problems like denial of service (DoS) attacks, routing attacks, Sybil attack etc. Key management protocols, authentication protocols and secure routing cannot provide security to WSNs for these types of attacks. Intrusion detection system (IDS) is a solution to this problem. It analyzes the network by collecting sufficient amount of data and detects abnormal behavior of sensor node(s). IDS based security mechanisms proposed for other network paradigms such as ad hoc networks, cannot directly be used in WSNs. Researchers have proposed various intrusion detection systems for wireless sensor networks during the last few years. We classify these approaches into three categories i.e. purely distributed, purely centralized and distributed-centralized. In this paper, we present a survey of these mechanisms. These schemes are further differentiated in the way they perform intrusion detection.

Keywords: Wireless Sensor Networks (WSNs), Intrusion Detection System (IDS), IDS agent installation.

1 Introduction

Wireless sensor networks (WSNs) are distributed, infrastructure-less, fault tolerant, scalable and dynamic in nature [1]. WSNs are vulnerable to several types of security threats that can degrade the overall performance of these networks. Key management, authentication protocols and secure routing protocols provide secure transmission while lacking reliable delivery of messages. In other words, these mechanisms can protect the network from outside attacks but show failure against inside attacks. They aim to provide data confidentiality, data authentication and data integrity. In an outside attack, when an intruder tries to get access to the data, these approaches hide secret information. In an inside attack, sensor node that is a part of the sensor network starts performing maliciously without trying to get access to the information present in the received messages. Roosta et al. [2] explain various possible attacks on wireless sensor networks i.e. denial of service, routing attacks, Sybil attack etc.

Intrusion detection system (IDS) is a security mechanism used to detect the abnormal behavior in the network. It is thought that intrusion detection systems are “not fit" for securing WSNs. This is true to some extent because IDS approaches are

D. Ślęzak et al. (Eds.): FGCN/ACN 2009, CCIS 56, pp. 234–241, 2009.

usually computationally expensive. But if we consider a WSN that works for tracking the movement of the enemy, this network can provide very useful information for making a strategy to beat the enemy in that area. Moreover, there is a rapid change in technology and keeping in mind the future perspectives; the capabilities of a sensor node will increase in near future. Sensor nodes will have more memory and survival time i.e. they might be used for transmitting multimedia information as well as for underwater applications. Due to the recent advancement in sensor technology, these networks will become visible and would be used by us in our daily life. Hence, there is a requirement of a secure WSN that ensures secure transmission and reliable delivery of packets in the network. IDS based mechanisms can be very effective to detect abnormal behavior of sensor nodes whether they cause DoS attacks, act as Sybil nodes or perform any other malicious activity.

In IDS, the unit that analyzes the network and detects abnormal behavior of node(s) is called an IDS agent. IDS agent collects network data for some time ‘t’, applies detection policy to detect abnormal activity and takes appropriate actions. Rajasegarar et al. [3] analyze several anomaly detection mechanisms in their work. Since 2005, researchers have proposed a number of IDS based security mechanisms that analyze the working of sensor node(s) and efficiently detect abnormal activities. They mostly target routing protocol attacks to explain their proposed methodology. Their work differ from each other in two ways i.e., installation of IDS agent, and the detection policy. There are three possibilities of installing an IDS agent; purely centralized, purely distributed and hybrid. In the first approach, it is installed at sink or BS only while in the second approach, IDS agent is present in every sensor node. In the third approach, monitor nodes are used for intrusion detection.

The rest of the paper is organized as follows: Section 2 contains a brief introduction of an IDS. We classify IDS based security mechanisms in Section 3 and explain each methodology. Finally, Section 4 concludes the paper.

2 Intrusion Detection System

Intrusion detection system (IDS) is a system that checks the network behavior and finds the nodes that are not working normally. It is an additional unit installed at the clients or server or both. This unit is called IDS agent. IDS agent works in three phases and each phase has a unit. *Collection unit* collects network data. *Detection unit* performs detection policy accordingly to find intrusions. *Response unit* generates alerts in case of abnormal activities.

2.1 IDS Agent Installation

IDS agent performs an important task for securing network from intrusive attacks. Researchers use three different ways of installing IDS agent in WSNs. These are; purely centralized, purely distributed and distributed-centralized.

Purely Distributed IDS Agent Installation Mechanism. In purely distributed IDS approach, IDS agent is installed in every node. It checks abnormal behavior of neighboring nodes locally. It analyzes the data that it receives from its radio range. There are further two ways for declaring a node as compromised or not. In *individualized decision making*, node that detects the anomalous behavior of another node sends that information to the sink or BS. In *cooperative decision making*, node that detects the anomalous behavior of any node communicates with other nodes and finally that node is declared compromised after voting.

Purely Centralized IDS Agent Installation Mechanism. In WSNs, sensor nodes sense the environment and transmit processed information to the sink or base station (BS). In purely centralized IDS approach, IDS agent is installed in the sink or BS. It requires an additional special routing protocol that gathers or collects information from nodes to analyze the behavior of sensor nodes collectively.

Distributed-Centralized IDS Agent Installation Mechanism. Cluster-head approach lowers the power consumption and efficiently reduces control overhead. The concept of monitor node is derived from this philosophy. In distributed-centralized approach, IDS agent is installed in monitor nodes only. This node performs two types of functions simultaneously. First, it performs activities like normal nodes and secondly, it checks for intrusion detection. The logic behind that approach is to minimize the detection overhead faced by purely distributed approach.

2.2 Detection Policy

In an intrusion detection system, detection of intrusion is the major phase. There are three different policies of detection; misuse detection, anomaly-based detection and specification-based detection.

Misuse Detection System. There are various attacks that follow same sequence of steps to launch its effect. In misuse detection system, these sequences of steps are used in order to detect these attacks. This detection mechanism is also called signature-based detection. It is like pattern matching. It works better for known attacks only but cannot cater unknown attacks.

Anomaly Detection System. Signature-based approach cannot detect attacks for which signature (known pattern) is not present. There are a number of attacks that change the signatures frequently. These attacks are hard to detect. Anomaly-based systems provide a security environment in which anything that deviates from the normal behaviour are declared anomalous or malicious.

Specification-based Detection System. Specification-based detection system works by defining rules for attacks. Sensor node's behaviour is checked against each rule sequentially. There is a failure bit associated with each node. If the sensor node violates any rule, failure bit is incremented. If number of failures of a particular node increases than a threshold after a time interval t; an alert about that node is generated.

3 IDS Based Security Mechanisms for Wireless Sensor Networks

Since recently, various intrusion detection systems have been proposed for detecting compromised node(s) in WSNs. We categorize these methodologies into three major classes depending upon the way they install IDS agent in the network.

3.1 Purely Distributed Approach

In purely distributed mechanisms, IDS agent is installed in each sensor node to analyze the working of other node(s).

Spontaneous Watchdog Approach. Roman et al. [4] introduce neighbor monitoring technique known as spontaneous watchdog. IDS agent also has two detection bodies; local agent and global agent. Local agent audits data that comes from those nodes that lie inside its radio range or are its neighbors. It generates alert if any node works abnormally, like flooding or if it receives message from a node that is not present in the neighbor list. On the other hand, node activates its global agent if it senses any communication in promiscuous mode. Here, global agent acts like a spontaneous watchdog. It checks whether nodes rebroadcast received message (s) or not.

Cooperative Local Auditing. Krontiris et al. [5] propose a specification based cooperative local auditing mechanism for detection of selective forwarding and black-hole attacks. They further extend their work for sink-hole attack in [6]. According to their approach, IDS agent is composed of five main components; local packet monitoring, local detection engine, cooperative detection engine, communication, and local response. The local packet monitoring component gathers packet from the radio frequency range of the node and transmits to the local detection engine. Specification-based detection mechanism is applied to find intrusions. In [5] and [6], they have mentioned four rules for detecting black-hole, selective forwarding and sink-hole attacks. Local detection engine performs this task. It checks whether packets of a particular node obey the rules or not. If it violates the specifications then an alert is sent to cooperative detection engine. This component then communicates with other nodes to check the status of that node among these nodes. If majority of the nodes validate the maliciousness of that node then an alert is passed to the local response about that node. There may be different types of responses to secure the network from that compromised node depending upon the configuration.

Fixed Width Clustering Algorithm. Another distributed anomaly detection mechanism is proposed by Loo et al. [7]. In this approach, twelve various features like number of packets received or sent or broadcast, route request sent or forwarded or received etc. are loaded. They are used to determine mean or standard deviation for each neighboring node in normal messaging. These values are normalized to get a single value. This value is utilized to form fixed width clusters. If it is close to any cluster central value, it is placed in that cluster. Otherwise, it forms another cluster and becomes a central value of that cluster. A range is also calculated for it. These values are also calculated by simulating various attack scenarios and are placed in the cluster. After analyzing these clusters, compromised nodes are detected. It is assumed that those clusters that have fewer points indicate the abnormal activity.

Artificial Immune System. Drozda et al. [8] propose an AIS based detection mechanism for wireless sensor networks because it is computationally less expensive and provides better detection performance. In this mechanism, system maintains a list of self-strings (normal behavior) and non-self strings (misbehavior). System learns normal behavior by maintaining strings called self-strings from the header of each received message. After that *random generate and test process* is introduced to form detector set. Self strings are compared with randomly generated strings. If newly produced string matches the self string, it is rejected; else, it is stored in the detector set. After that new strings are again randomly produced. This time, they are compared with detector set entities. If match appears, it confirms a non-self string and it is stored in the list of non-self string. This process is called negative selection because it determines those behaviors (strings) that are used for determining abnormal activity. When this process completes, attacks are launched to analyze the false positive rate.

Intrusion-aware Validation Algorithm. It enhances those distributed cooperative IDS systems that lack confirmation about the source of the alert because compromised nodes can generate false alarms about normal node(s) [9]. It works in two phases. In *consensus phase,* node checks after receiving any alert about occurrence of malicious activity that whether it is any declared (available in list) abnormal node or not. If the information is not available then it checks the anomaly type and the threat level. It randomly selects n number of neighbors, according to the threat level, for consensus and sends confirmation request packet(s). When any node receives confirmation request packet, d*ecision phase* activates. Neighbor node replies with three types of responses: 1 agrees with claim, 0 don't know and -1 does not agree with claim. Sensor node takes decision on the basis of the responses received from the randomly selected nodes. There are three possible decisions; validate (node is abnormal), no consensus (not identified) and invalidate (node that sends the alert is compromised).

Pair-based Abnormal Node Detection. Ahmed et al. [10] propose a novel distributed abnormal node detection technique. It uses both signature and anomaly based techniques to identify compromise node. In this technique, sensor network is divided into pairs that further lead to form groups. These groups communicate with each other in hierarchical way. They are controlled by central pairs or cluster-heads. Every sensor node analyzes behavior of its pairing node. It has a local detection engine and a local knowledge base while there are two central containers; central knowledge base and central signature key management engine. *Central signature key management engine* is responsible for secure transmission of messages between the pairs and groups. Data is collected based on some predefined features by the local knowledge base about pairing node and is used by the local detection engine to detect the anomaly. C*entral knowledge base* collects and stores information about all the nodes present in the group or outside the group. The information updates frequently and it shares the relevant information about the nodes with individual node. Node performs anomaly detection to generate alert about the pairing node, if it is found abnormal. This updates the central knowledge base too.

3.2 Purely Centralized Approach

In this approach, the sink or the base station collects some specific information from sensor nodes using any special routing protocol and analyzes it to detect intrusions.

ANDES. Gupta et al. [11] present a centralized anomaly detection mechanism for detecting fail-stop failures and several routing protocol attacks. It works in two main phases i.e. collection of information and detection. ANDES gathers information from the sensor network using two sources; data plane (normal or regular collection of data in the sensor network) and management plane (specific information from sensor nodes using a specialized routing protocol). Sink or BS collects sufficient information before applying anomaly detection. ANDES consist of three main components. *Collection of application data* collects regular data. *Collection of Management information* uses an additional management routing protocol to collect address, parent, hops, send_cnt, receive_cnt, fwd_cnt, etc from each node after an interval of time. *Detection policy* works in three phases; analysis of application data, analysis of management data and cross checking to determine the root cause of the attack.

Application Independent Framework. Zhang et al. [12] present simple graph theory based approach that efficiently detects compromised beacon nodes. Beacon nodes provide location information to the sensor nodes. It is assumed that IDS agent is installed at beacon nodes. It produces alerts about the maliciousness of sensor nodes. A compromised beacon node transmits false information about other nodes and degrades the performance of the routing protocol. It is not a pure centralized IDS methodology. It is centralized-distributed because beacon nodes generate alerts about the malicious activity. Sink or BS receives these alerts by any secure transmission protocol. Once efficient amount of data is gathered, it applies the proposed graph theory based detection mechanism to find whether information is received from reliable source or not.

3.3 Distributed-Centralized Approach

IDS agent is installed in some nodes called monitor nodes. Monitor node listens in two modes i.e. normal and promiscuous. In normal listening, monitor node interprets and forwards after processing (application dependent) those messages that are destined to it. In promiscuous listening, monitor node interprets all messages whether they are destined to it or not. They avoid the complexity of using an additional specialized routing protocol (purely centralized) and limit the overall energy consumption of sensor nodes (purely distributed).

Decentralized Intrusion Detection Model. Da Silva et al. [13] present a specification based distributed centralized IDS mechanism. IDS agent is installed in monitor node. It works in three phases. In *Data Acquisition*, monitor node listens in promiscuous mode and maintains an array data structure for each node. This contains information about those nodes that lie in the neighborhood. In *rules application*, monitor node checks whether any node violates any rule or not, after collecting sufficient amount of data in the first phase. Several rules or specifications are discussed i.e. retransmission rule for selective forwarding or black-hole attack, repetition rule for flooding etc. There is a failure counter for each node. If a node's data structure violates any rule, its respective counter is incremented. In *intrusion detection*, monitor node evaluates failure history table of each node. If counter value exceeds from certain threshold ‘th’ in time interval t, an alert is generated.

Cumulative Summation. Phuong et al. [14] propose an anomaly-based distributed centralized detection mechanism to analyze the behavior of nodes. It secures wireless sensor network from three categories of attacks. These are 1) Compromised nodes attract the attention of other nodes i.e. black-hole, sink-hole or worm-hole attack 2) Affects message like collision 3) Flooding to exhaust resources. Cumulative Summation (CUSUM) works in two phases. In *data acquisition*, monitor node maintains a table containing total number of incoming packets and outgoing packets that relate to neighbor n (1, 2, 3... N). In *anomaly detection*, CUSUM works on the collected data to detect three changes; amount of messages received or collision occurrence with the packets or number of packets emerging from a particular node. If these values are above certain threshold, an alert is generated.

Table 1. IDS based security mechanisms

Proposed Approach	Detection Policy	Decision	Attacks
Spontaneous Watchdog [4]	Any	Individual	Novel
Cooperative local audit [5]	Specification-based	Cooperative	Routing
Fixed-width clustering [7]	Anomaly-based	Individual	Routing
Artificial Immune System [8]	Anomaly-based	Individual	MAC/Routing
Intrusion-aware validation [9]	Anomaly-based	Cooperative	-------
Pair-based approach [10]	Both	Pairing node	Novel
ANDES [11]	Anomaly-based	Sink or BS	Phy./Routing
App. Independent Framework [12]	Anomaly-based	Sink or BS	-------
Decentralized IDS [13]	Specification-based	Monitor node	Trans./Routing
Cumulative Summation [14]	Anomaly-based	Monitor node	Trans./Routing

4 Conclusion

In this paper, a detailed discussion and analysis of the existing Intrusion Detection Systems (IDS) for Wireless Sensor Networks is presented. IDS is an essential part of security for every network. Energy-efficient intrusion detection systems are suitable for wireless sensor networks. Purely centralized IDS approaches are power efficient because the most powerful part of the network (sink or BS) detects intrusion. But, these techniques are complex and require some specialized routing protocol that gathers data from each sensor node to BS or sink for anomaly detection. On the other hand, purely distributed IDS techniques are not energy-efficient because IDS agent is installed in every node. It increases extra computation or power consumption at node level. Distributed-centralized IDS approach suits WSNs in accordance with energy consumption and complexity; but it has its own constraints. Wireless sensor networks are vulnerable to a number of inside attacks that affect the overall performance of the network. These attacks results in wrong interpretation of the sensor field. There is a requirement of an energy-efficient intrusion detection system that works in distributed manner and cooperates with other nodes to identify the abnormal behavior of nodes.

References

1. Akyildiz, I.F., Su, W., Sankarsubramaniam, Y., Cayirci, E.: A Survey on Sensor Networks. IEEE Communication Magazine, 102–114 (2002)
2. Roosta, T., Shieh, S.P., Sastry, S.: Taxonomy of Security Attacks in Sensor Networks and Countermeasures. In: Proc. of 1st IEEE Int. Conf. on System Integration and Reliability Improvements (2006)
3. Rajasegarar, S., Leckie, C., Palaniswami, M.: Anomaly Detection in WSNs. In: IEEE Wireless Comm., Security in Ad hoc and Sensor Networks, pp. 34–40 (2008)
4. Roman, R., Zhou, J., Lopez, J.: Applying Intrusion Detection Systems to WSNs. In: IEEE Consumer Communications and Networking Conference, vol. 1, pp. 640–644 (2006)
5. Krontiris, I., Dimitriou, T.: Towards Intrusion Detection in Wireless Sensor Networks. In: Proc. of 13th European Wireless Conference, Paris, France (2007)
6. Krontiris, I., Dimitriou, T., Giannetsos, T., Mpasoukos, M.: Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks. In: Kutyłowski, M., Cichoń, J., Kubiak, P. (eds.) ALGOSENSORS 2007. LNCS, vol. 4837, pp. 150–161. Springer, Heidelberg (2007)
7. Loo, C.E., Ng, M.Y., Leckie, C., Palaniswami, M.: Intrusion Detection for Routing Attacks in Sensor Networks. International Journal of Distributed Sensor Networks 2(4), 313–332 (2006)
8. Drozda, M., Schaust, S., Szczerbicka, H.: Is AIS Based Misbehavior Detection Suitable for Wireless Sensor Networks? In: Proc. of IEEE Wireless Communications and Networking Conference, Hong Kong, pp. 3130–3135 (2007)
9. Shaikh, R.A., Jameel, H., Auriol, B.J., Lee, S., Song, Y.J.: Trusting Anomaly and Intrusion Claims for Cooperative Distributed Intrusion Detection Schemes of WSNs. In: Proc. of International Symposium on Trust Computing, China, pp. 2038–2043 (2008)
10. Ahmed, K.R., Ahmed, K., Munir, S., Asad, A.: Abnormal Node Detection in WSN by Pair Based Approach using IDS Secure Routing Methodology. International Journal of Computer Science and Network Security 8(12), 339–342 (2008)
11. Gupta, S., Zheng, R., Cheng, A.M.K.: An Anomaly Detection System for Wireless Sensor Networks. In: Proc. of IEEE International Conference on Mobile Ad hoc and Sensor Systems, pp. 1–9 (2007)
12. Zhang, Q., Yu, T., Ning, P.: A Framework for Identifying Compromised Nodes in WSNs. ACM Transaction Information System Security 11(12) (2008)
13. Da Silva, A.P.R., Martins, M.H.T., Rocha, B.P.S., Loureiro, A.A.F., Ruiz, L.B., Wong, H.C.: Decentralized Intrusion Detection in WSNs. In: Proc. of the 1st ACM Int. workshop on Quality of service & security in wireless networks, Canada, pp. 16–23 (2005)
14. Phuong, T.V., Hung, L.X., Cho, S.J., Lee, Y.K., Lee, S.: An Anomaly Detection Algorithm for Detecting Attacks in WSNs. In: Mehrotra, S., Zeng, D.D., Chen, H., Thuraisingham, B., Wang, F.-Y. (eds.) ISI 2006. LNCS, vol. 3975, pp. 735–736. Springer, Heidelberg (2006)