A Comprehensive Review of Intrusion Detection Systems for Wireless Sensor Networks

WARDA AHMAD, SIDRA ANWAR, YASIR SALEEM*, JUNAID ARSHAD, KHAWAR BASHIR, HAFSA TAHIR

Department of Computer Science and Engineering, University of Engineering and Technology Lahore, Pakistan
**Corresponding author's e-mail: ysaleem@gmail.com*

(Received on 7th June, 2016 Accepted on 1st August, 2016)

Abstract

Wireless Sensor Networks (WSNs) are gaining wide spread acceptance in the regimes where close communication with physical world are important. Due to importance in almost all fields of practical life WSN are vulnerable to wide range of attacks. Securing the network from those attacks is a vital task in order to achieve the required performance. Intrusion Detection Systems (IDS) are security mechanisms against network vulnerabilities. The purpose of this paper is to compare and evaluate most recently proposed IDS methods in WSNs and identifying their strengths and weaknesses.

***Keywords*:** Intrusion detection system, Wireless sensor network, Energy consumption, Detection rate, Review

INTRODUCTION

Wireless sensor networks (WSNs) are types of networks which consist of hundreds of thousands of tiny nodes. These nodes are sensing devices also called motes. These motes generate data as well as they act as network relays. Each of these motes/nodes consists of a transceiver, sensor(s) and a microprocessor. These motes are designed to consume low power to extend their life-time up to several months and years. Their processing capability is also low because they only sense data like temperature, heat, humidity etc from the physical world and send this information to the main system for further processing. Some motes have on-board microprocessors which initially process data before sending it to macro processor. They also have low cost. They have a testing issue in making productive self-organized WSN, on the grounds that sensor nodes are circulated in wide area [1].

One of the important things is that WSN should be adaptable, dependable, self-organized and secure and have flaw resilience. Due to the low cost and straightforward proliferation attributes of wireless sensor networks, they have wide spread applications in many fields of science, military and health. Some of their uses include sensing and accumulating information regarding different exercises, case investigation of war zone (e.g. Boomerang Sniper Identifying System), distinguishing NBC (Nuclear, Biological, Chemical) assaults, observing parkway movement, learning natural life and seas (Great Duck Island - GDI Project), fire alert framework, home automation systems, agriculture, transportation and space investigation to name a few [2].

Due to these vast applications of WSNs they are more vulnerable to intrusion attacks. The security of WSNs is very critical task because of their self-organizing nature, dependency on the other nodes, limited bandwidth, low battery power [3]. There are two types of mechanisms which give security to the network. These are prevention based and detection based. Prevention based mechanisms provide confidentiality, integrity and authentication security which include cryptography, secure routing, key management and so on. All these are known as first line security mechanisms. The second is detection based mechanisms which includes IDS. This is said to be second line security mechanism for the network [4].

Intrusion is a process of sending malicious software to the network or hijacking a network. Intrusion detection is a system which is used to detect the intrusion attacks on wireless sensor networks. In 2015 many intrusion attacks were done on very popular networks .The most common and devastating attack is cyber-attack like the one on French television network TV5Monde on 8th April, 2015. Another attack was on US power grid on Oct 21, 2015 and many others. Due to this, an Intrusion detection system plays very important role.

One of the major issues in the implementation of IDS to wireless sensor network is to choose the type of strategy that consumes less power in WSN. The reason being that each node of WSN has low powered battery, limited computation capability and very less storage available. Intrusion detection systems are computationally expensive and they are made for wired and ad hoc network so they are not directly applied to these wireless sensor networks.

In this paper, we present a comprehensive review of recent intrusion detection system models for wireless sensor networks. The section named Intrusion Detection System (IDS) in Wireless Sensor Networks gives an overview of IDS in wireless sensor networks. In this section we have described some basic intrusion detection methodologies

The next section presents the related work done in this field. After this the review of some recent IDSs for wireless sensor network has been presented. Analysis and comparison of these IDSs is presented in the next section. This section also discusses some strengths, weaknesses and future work of the analyzed IDSs. Finally, the last section closes the paper with a conclusion.

Intrusion Detection System (IDS) in Wireless Sensor Networks

In the network or a system intrusion is the process of gaining unauthorized access and then performing unauthorized activity. Intrusion is done by two methods; first one is known as passive intrusion which includes eavesdropping and Information gathering the second one is known as active intrusion like packet dropping, malicious packet forwarding, hole attacks etc. For these types of intrusion attacks first line of security system i.e. Intrusion prevention is not sufficient. So there must be the second line of security system i.e. Intrusion detection [5].

IDS is said to be the second line of security in any security system. It means it detects the intrusion activity (active or passive), type of intrusion (warm hole, black hole, sink hole etc) and protocol layer at which intrusion occurs. It also detects the intruder i.e. location of intruder. All of this information is very useful for mitigating the intrusion by placing appropriate controls. Hence Intrusion detection system (IDS) is a hardware or software system, used for detection of attacks whether they are internal or external attack. IDS have four main components: sensor, detector, knowledge base and response component. Sensor collects the data. Then this collected data is analyzed by the detector with the help of knowledge base because knowledge base contains all the signatures of serving attacks. And then response component manages the response given by the detector on the basis of information in knowledge base [2].

IDSs are classified on many bases which are given below:

A. Source of audit data

It means that from which location the data is to be analyzed. On this base IDSs are classified into three types.

- Network Base Intrusion Detection System (NIDS)
- Host Based Intrusion Detection System (HIDS)
- Hybrid Intrusion Detection System

NIDS is systems which captures network traffic on the specific network with the help of sensors and then analyze this traffic and detect the intrusion attacks like DoS attack, Port scans etc. It analyze the packets and their headers to find out any malicious signature present in them [6]. HIDS is a system which detects those attacks which are inside the system. It maintains the log information of the system then by analyzing this find out attack. Hybrid intrusion detection system is the combination of both above systems.

B. Detection methodologies

There are three basic detection methodologies used by intrusion detection system.

1) *Anomaly based detection:* In this type of detection technique IDS tries to analyze the normal operation of the system. The normal performance of the system is profiled and any deviation from the normal is said to be anomaly. This is a runtime detection technique. Anomaly base detection is classified in three categories on the basis of nature of their processing. Statistical based (Uni-variant, multi variant, time series model), Knowledge based (Expert system, UML, FSM), Machine learning based (Markov model, Fuzzy logic, Neural Network) [5,8].
2) *Specification based intrusion detection:* In this technique manually some specifications and limitations are designed and then the behavior of the system is monitored. It is similar to anomaly based detection but the difference is that its specifications are manually designed [5].
3) *Misuse based (ruled based) detection: In* this detection type profile of known attacks are managed. And on the basis of this log attacks are detected. This approach is very useful and it has lowest false positive rate. Advantage of this technique is that it can easily find out the known attacks. The main disadvantage of this attack is that if the attack occur whose signature is not present in profile than this attack will be difficult to detect [7].

C. Executing location of the gathered data

On the bases of executing location IDSs are divided into four types: Centralized IDS, Stand-alone IDS, Distributive and Cooperative IDS and Hierarchal IDS. Centralized IDS are those systems which monitor all the activities in the network and find intrusions in the monitored data. Stand-alone IDS are the systems which run independently on each node, collect their own data then make decisions. Distributive and Cooperative IDS is proposed for flat networks. Each node collect data individually and if node detects the intrusion it sends report to the cooperate network. Hierarchal IDS is developed for multilayer architecture networks [2].

Related Work

Recently, much work has been done on intrusion detection systems in wireless sensor networks. A few surveys have already been published in order to review the existing work. Some of which are presented here.

An overview of security attacks in wireless sensor network has been presented in an article [8] and also the models and architectures of some of the intrusion detection system (IDS) in wireless sensor network is studied in this article. A comparison and characteristics of different IDS models have also been presented in this paper.

Another study conducted by Robert Mitchell and Ing-Ray Chen provides a survey of intrusion detection in wireless sensor networks. This study classifies the existing wireless intrusion detection system (IDS) techniques based on collection process, analysis technique, detection technique, and trust model and target wireless network. It then summarizes the advantages and disadvantages of these wireless intrusion detection system techniques with respect to specific parameters of target wireless networks and finally suggests some future research areas [7].

A survey of Intrusion Detection Systems (IDSs) for wireless sensor network is conducted in an other article[5]. This paper first provides the detailed information about IDSs, and then provides a survey of IDSs proposed for Mobile Ad-Hoc Networks. After that IDSs proposed for wireless sensor networks are discussed. Further in this study, the analysis, comparison and strengths and weaknesses of each system are discussed in detail.

Similarly another study presents a survey of IDSs in wireless sensor networks (WSNs). This study also presents the cyber-attacks occurring in wireless sensor networks in detail. As the features of wireless sensor networks are different from wired networks and non-energy constrained wireless networks, so intrusion detection systems in wireless sensor networks behave differently and also take different approaches to detect the intrusions. In this study, these approaches are discussed in detail [2].

Another article related to this study first provides a review of some of the existing intrusion detection systems for wireless sensor networks. Then in this study, a new intrusion detection system is proposed named as Insomnia Mitigating Intrusion Detection System (IMIDS). IMIDS is a cluster based layered model that can efficiently reduce sleep deprivation attack in wireless sensor networks [9].

Recently Proposed IDSs for WSNs

Since security threats for WSN are different from wired networks due to the limited energy and storage constraints, therefore IDS for WSN are designed accordingly. In this section we have briefly discussed the most recent IDSs for WSNs based systems. The systems included for review are as follows:

- A Global Hybrid Intrusion Detection System for Wireless Sensor Networks
- Distributed Detection of Flooding and Gray Hole Attacks in Wireless Sensor Network
- An Improvised Hierarchical Black Hole Detection Algorithm in Wireless Sensor Networks
- Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Networks
- Insomnia Mitigating Intrusion Detection System (IMIDS)

A. A Global Hybrid Intrusion Detection System for Wireless Sensor Networks.

A Hybrid Intrusion Detection System (HIDS) using Support Vector Machines (SVM) as learning algorithm and attack signatures for detection is introduced in Figure 1 [10]. A cluster based topology is used, where one known node is designated as the Cluster Head (CH) which collects data from all other sensors in the cluster and sends the aggregated data to the base station. The network lifetime can be increased by the use of CH, by lowering the energy consumption of network. The architecture of the system is given in Figure 1.

A Cluster Head is selected on the basis of its energy. The residual energy of CH is calculated by the following formula:

$$V_i(t) = [Initial - E_i(t)] / r$$

Where Initial = initial energy, Ei(t) = residual energy, and r = current round of CH selection. The process of CH selection is announced by the Base Station (BS), which then calculates the average deviation and values of the energy data. The old CH announces the end of its authority while the new CH sends alert messages to the nodes. All members of the cluster are authenticated by the CH, which is in turn authenticated by the BS. Due to energy constrains in the network nodes, agents are activated only when required.

SVM is used as a method of anomaly detection, which is suitable for detection of small sample data. Since IDS data is large in size, therefore during the training phase the data collected from all layers of system is sorted and pre-processed offsite, where enough resources are available. The training data then goes through a data reduction phase, which reduces the size of data so that it can be further processed by the SVM. A maximum margin linear hyper plane is defined by the SVM after mapping the training data. Given the training set for the sample set *(x_i, y_i):*

$$i = 1 \ldots\ldots, n,\ x \text{ €} R^d\ y \text{ €} ||+1, -1||$$

Where ||+1|| is normal, and ||-1|| is abnormal, the classify hyper plane equation is given as

$$w \,.\, x + b = 0$$

Here *w* represents a normal vector and offset is given by the parameter *b*. The Support Vectors are the training samples on the hyper plane. In context of this scheme, the vectors of each node are sent to its one-hop neighbor, and the final hyper plane is calculated discriminator for all nodes separating data into two classes.

The signature based model uses discovery protocol employing signatures for the detection of harmful nodes and protect network against attacks by these nodes. Based on a set of rules, this protocol defines the behavior of the target as either normal or abnormal. This system has used four types of rules for detecting following attacks:

- Selective forwarding attack
- Black hole attack
- Hello flood attack
- Wormhole attack

The decision making model uses the following set of rules to take proper action for a given situation:

- If SVM detects an attack and signature model does not detect the attack, then it is classified as an error or false alarm

- If both SVM and signature model detect an attack, then it is classified as an attack.

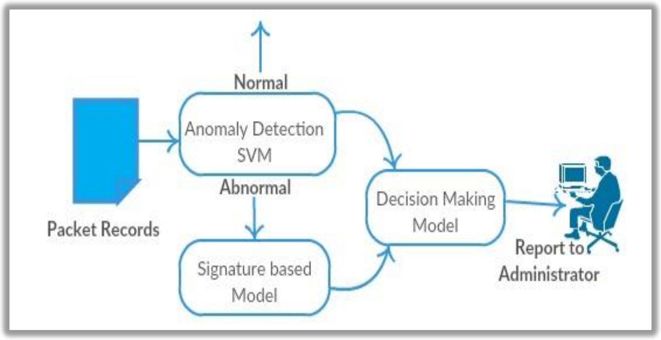

Figure 1: A Hybrid IDS for Wireless Sensor Networks

B. Distributed Detection of Flooding & Gray Hole Attacks in Wireless Sensor Network

In [11], authors have discussed the main types of Denial of Service (DoS) attacks i.e. flooding, gray hole and black hole, with respect to the energy consumption and have given a methodology to prevent these types of attacks in the WSN. Energy consumption is a critical issue to be addressed for WSN and appropriate measures should be taken to conserve energy.

The proposed system uses cluster heads (CH) to perform the intrusion detection procedure for identification and isolation of attacker nodes responsible for the DoS attack. A predicted energy value for all the nodes in the cluster is given by the CH and the value of actual energy consumed by the node is obtained from all the nodes. Anomaly in the predicted and actual value determines an attack.

The system is assumed to consist of homogenous WSN, in which all nodes have the same energy initially. The residual energy of all nodes is sent to the CH after regular intervals, which is used to calculate actual energy. The formulas for actual energy and predicted energy are given as follows:

$$\text{Actual energy } (E1(v))=\text{Initial energy}-\text{Residual energy}$$
$$\text{Predicted Energy } (Ek+1(v))=ek+\text{Ø}(Ek(v)-Ek\text{-}1(v))$$

Whenever the selection of new cluster head takes place, the newly elected CH get the routing table from the previous one, which contains the energy information about the nodes in the cluster. The actual energy consumption can be determined from the difference of energy levels between two intervals. The mismatch of predicted and consumed energy of a node is considered as a malicious node. If calculated energy is greater than predicted energy, then the node is launching a flooding attack because sending large number of packets requires abnormally high amount of energy. Gray hole attack is detected in the opposite case i.e. when predicted energy is greater than calculated energy as selective number of packets are dropped by the attacker node; hence decreasing the transmission. By using the above system, the malicious nodes causing flooding and gray hole attacks are detected efficiently. The system is consuming less energy, and is thus lightweight.

C. An Improvised Hierarchical Black Hole Detection Algorithm in WSNs.

Black hole attacks are one of the most harmful types of routing attacks on the network layer. These attacks aim for the Cluster Heads (CH), by designating a malicious node as CH and absorbing all the data from other nodes in the cluster. The malicious node presents itself as the shortest route, and thus absorbs all the received messages and performs selective forwarding. The system proposed in [12] prevents black hole attack by implementing a simple strategy where each node sends a control packet to CH and one of the agents at the end of each transmission. The control packet consists of identity of the node and the number of packets received by the CH (Nbpkr) [12]. The flow chart of the proposed algorithm is given in Figure 2 [12].

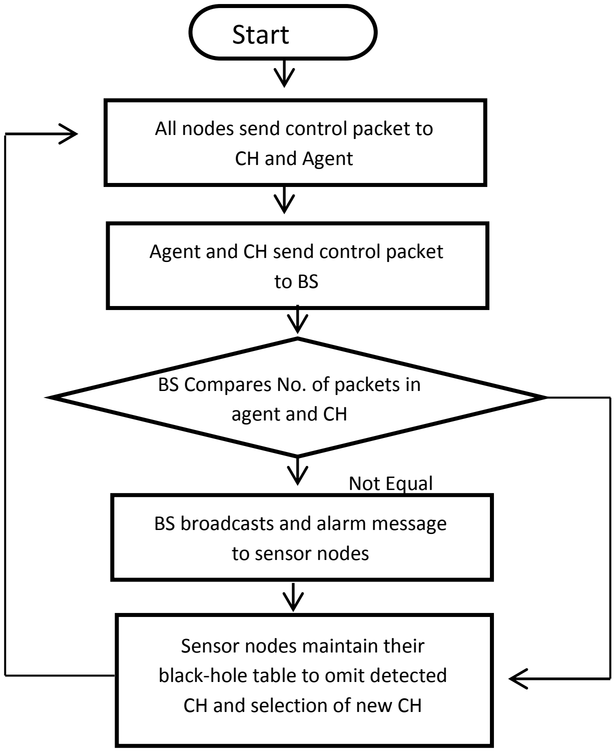
Start
All nodes send control packet to CH and Agent
Agent and CH send control packet to BS
BS Compares No. of packets in agent and CH
Not Equal
BS broadcasts and alarm message to sensor nodes
Sensor nodes maintain their black-hole table to omit detected CH and selection of new CH

Figure 2: Flow Chart for Black Hole Detection Algorithm

The difference in the Nbpkr and number of packets sent by the agent and CH to the base station determines the presence of black hole attack. In case of attack presence, an alarm packet containing the identity of the malicious node is sent to all nodes by the base station. A black hole table is maintained by each node which helps in the selection of new CH by preventing malicious node from getting selected as CH again.

D. Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Networks

The system proposed in [13] defines an IDS based on abnormal behaviors and traffic signatures to define attacks on the network. The system uses a network based approach suitable for WSN. There are two types of network nodes in the system. Those nodes which are deployed with network based IDS (NIDS) act as watchdogs for identification of possible attacks by eavesdropping on the packets exchanged between neighbor nodes acting as host based IDS (HIDS). A set of rules is organized on each NIDS which matches the monitored messages with rules, and if the match occurs it generates an alarm and sends it to the Event Management System (EMS). The nodes with maximum number of alarms is detached from network and designated as a compromised node.

The authors in this paper have considered a heterogeneous WSN system; therefore each NIDS has different set of rules based on the neighborhood nodes. A policy programming approach is adopted by the authors for this purpose. A predefined role group is required in order to classify different rules for each of the traffic type in WSN. Each rule is transmitted via configuration channel to NIDS nodes.

The Event Management System (EMS) runs on the sink node, with no restraints on energy and high processing capabilities. Its function is collection of data from NIDS and its comparison in order to identify the compromised nodes or intruders. The system consists of the following three modules:

1) *Packet Monitoring Module***:** It collects the communication data from nodes within range of NIDS. Due to memory constraints, not all the eavesdropped packets are stored. Each packet is stored in the temporary buffer for applying rules, after which it is discarded.
2) *Detection Module:* this module is responsible for the alarm triggering by storing, management and application of rules specified by the administrator. The analysis of network traffic at discrete locations helps improving the performance.

3) *Action Module:* It sends an alert to EMS whenever an intrusion is detected by NIDS in the neighborhood. The administrator can then compare the alert with alert messages sent by other NIDS for the same node and takes action accordingly.

E. Insomnia Mitigating Intrusion Detection System (IMIDS)

Insomnia Mitigating Intrusion Detection System (IMIDS) is proposed to detect sleep deprivation attack in heterogeneous wireless sensor network. A sleep deprivation attack is an attack in which intruder forcefully awake the sensor nodes until they can consume their energy. After that sensor nodes stop working and their sleep cycles are disturbed. In this case, the lifetime of sensor node is minimized. IMIDS uses cluster based mechanism in which each sensor network is first divided into clusters which are further subdivided into sectors. The objective of using the cluster based mechanism is to reduce the network energy consumption in an efficient manner. The block diagram of sensor network is shown in Figure 3 [9].

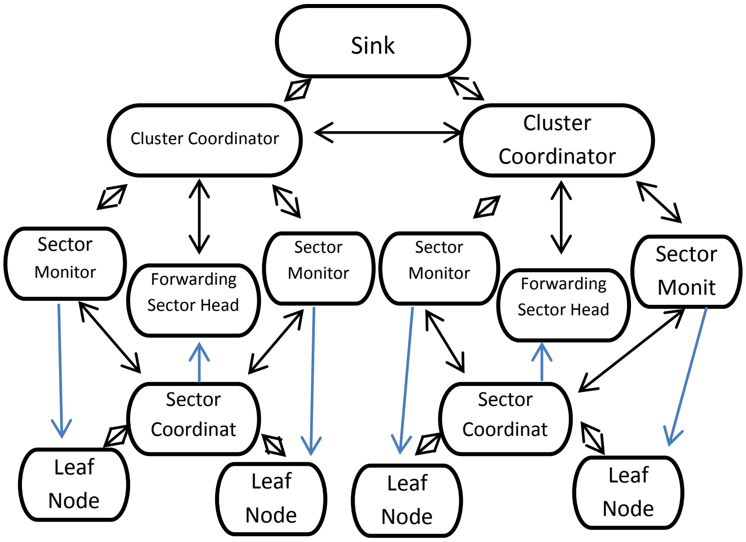

Figure 3: IMIDS Layered Model

It consists of five layers. The description of each layer is given below.

1) Layer 1 is the lowest layer of the sensor network. It consists of the Leaf sensor nodes that detect the data and send it above to the layer 2.

2) Every sector in layer 2 has a sector coordinator that receives the data sent by the layer 1. Layer 2 also has a capacity to detect anomaly. The purpose of sector coordinator is to keep the list of all leaf nodes in a sector. Sector coordinator also separates the suspected nodes from the valid nodes. The detail of suspected nodes is saved in suspected list and forwarded to the sector monitor while valid nodes are sent to the forwarding sector head of the above layer.

3) Elements of layer 3 are forwarding sector head and sector monitor. Forwarding sector head adds the detail of valid packet to the forwarding table and sends the valid data to the cluster coordinator. While sector monitor takes the data of the suspected nodes from layer 2, detects the intruders and compromised nodes and adds their details in quarantine list. Finally it sends the data to the cluster coordinator of layer 4.

4) Every cluster in layer 4 has a cluster coordinator which is used to monitor the forwarding sector head and sector monitor of each sector in a cluster. Cluster coordinator adds the detail of valid packets into the valid list and sends valid data to the sink node. Two or more cluster coordinators also interact with each other to form a global intrusion detection system.

5) Layer 5 is the upper Layer of the IMIDS layered model. It has a sink node that takes data from layer 4 and acts as an access point or a gateway between sensor networks and other networks. Sink node also saves the backup data of all clusters [9].

Comparison and Analysis of Recently Proposed IDSs

In this section, we have compared and analyzed the intrusion detection system models discussed in previous section. The analysis is done on the basis of some parameters. These parameters are detection rate, false positive rate, technique used and energy consumption. Detection rate and false positive rate is defined as follows:

Detection Rate: The number of the detected attacks divided by the total number of attacks.

False Positive Rate: The number of normal connections classified as an anomaly divided by the total number of normal connections (patterns).

An IDS model should have high detection rate, low false positive rate and should also have a low energy consumption to perform efficiently and to maximize its lifetime.

Comparison and analysis of our discussed IDSs is shown in Table1 while Table 2 shows the pros and cons and future work of these analyzed IDSs.

Table 1: Analysis and Comparison of IDSs

Intrusion Detection Systems (IDSs)	**Parameters**			
	Detection Rate	**False Positive Rate**	**Technique used**	**Energy Consumption**
Global Hybrid IDS	Almost 98%	Near 2%	Anomaly detection with SVM and signature based	Low, energy consumption is reduced by using cluster head
Distributed Detection of Flooding and Gray Hole Attacks	High	No evaluation regarding false positive rate is found	Learning based energy prediction algorithm	Low, Energy consumption is determined by calculating the difference of energy levels between two time intervals
An Improvised Hierarchical Black Hole Detection Algorithm	High	No evaluation regarding false positive rate is found	Rule based technique	Energy Consumption is 50mj for 20 nodes and it is less than as compared to other existing algorithms
Policy and Network-based IDS	High	No evaluation regarding false positive rate is found	Rule based technique	No evaluation is found
Insomnia Mitigating IDS	Detection Accuracy is 100% for 20 monitor nodes	No evaluation regarding false positive rate is found	Anomaly detection technique	Energy consumption with clustering is less as compared to without clustering

Table 2 Pros, Cons and Future Work of Intrusion Detection Systems

IDS	Pros	Cons	Future Work
Global Hybrid IDS	High Detection Rate, Low False Positive Rate, Low Communication Cost, Lift time of network is increased	None	Detailed simulation of different attacks needs to be performed
Distributed Detection of Flooding and Gray Hole Attacks	High detection ratio, Life time of network is increased, Low computation complexity, Faster intrusion detection	None	Detailed analysis of algorithm needs to be performed
An Improvised Hierarchical Black Hole Detection Algorithm	Efficient algorithm, Save the network from black hole attack, Improves the node security	It mostly emphases on black hole attack, The model used in this algorithm is comprehensive and complex hence computation complexity is increased.	Simulation of sensor nodes as black hole nodes along with cluster head can be conducted.
Policy and Network-based IDS	Detect and reports the security attacks	It cannot detect the wireless channel dynamically	Optimization of process is needed to store the new detection rules
Insomnia Mitigating IDS	Low energy consumption, Maximize the life time of network, High detection rate	It only detects the sleep deprivation attack	No future work is found

CONCLUSION

Wireless Sensor Networks (WSNs) are the large scale networks which consist of the hundreds of thousands of small nodes. The security of WSNs is very critical issue because of their self-organizing nature, dependency on the other nodes, limited bandwidth, and low battery power. To secure and prevent the network from intrusions, different intrusion detection systems (IDSs) are used. In this paper, we have presented the survey of recent intrusion detection systems (IDSs) for wireless sensor networks. We have first discussed the intrusion detection systems (IDSs), their classification and some detection methodologies. Then we have presented the review of some recent intrusion detection systems for wireless sensor network. Finally, we have summarized the analysis, comparison and pros and cons of these IDSs in tabular form.

REFERENCES

[1] I. F. Akyildiz and M. C. Vuran, *Wireless Sensor Networks* vol. 4: John Wiley & Sons, 2010.

[2] O. Can and O. K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," in *Proc. 6th Int. Conf. Modeling, Simulation Appl. Optimization (ICMSAO)*, 2015, pp. 1-6.

[3] N. A. Alrajeh, *et al.*, "Intrusion detection systems in wireless sensor networks: A review," *Int. J. Distributed Sensor Networks*, vol. 2013, pp. 1-7, 2013.

[4] S. Shen, *et al.*, "Signaling game based strategy of intrusion detection in wireless sensor networks," *Comput. Math. Applicat.*, vol. 62, pp. 2404-2416, 2011.

[5] I. Butun, *et al.*, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tutorials*, vol. 16, pp. 266-282, 2014.

[6] L. Koc, *et al.*, "A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier," *Expert Syst. Applicat.*, vol. 39, no. 18, pp. 13492-13500, 2012.

[7] R. Mitchell and R. Chen, "A survey of intrusion detection in wireless network applications," *Comput. Commun.*, vol. 42, pp. 1-23, 2014.

[8] Y. Maleh and A. Ezzati, "A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks," *CoRR*, vol. abs/1401.1982, no. 2014.

[9] T. Bhattasali and R. Chaki, "A survey of recent intrusion detection systems for wireless sensor network," in *Advances Network Security Applicat.*, D. C. Wyld, *et al.*, Eds., ed: Springer Berlin Heidelberg, 2011, pp. 268-280.

[10] Y. Maleh, *et al.*, "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks," *Procedia Comput. Sci.*, vol. 52, pp. 1047-1052, 2015.

[11] N. Dharini, *et al.*, "Distributed detection of flooding and gray hole attacks in Wireless Sensor Network," presented at the 2015 Int. Conf. Smart Techn. Management Comput., Commun. Controls, Energy Materials (ICSTM), Avadi, Chennai, India, 2015.

[12] A. B. Karuppiah, *et al.*, "An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks," presented at the 2015 Int. Conf. Innovation Inform. Comput. Techn. (ICIICT), 2015.

[13] J. P. Amaral, *et al.*, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks," presented at the 2014 IEEE Int. Conf. Commun. (ICC), 2014.