IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

Trust Based Approaches of Intrusion Detection Architecture for Wireless Sensor Networks: A Survey

Jeelani[1], Manoj Rana[2], Subodh Kumar[3] and Aasim Zafar[4]

Department of Computer Application, IET, Mangalayatan University, Aligarh, India[1,2,3]

Department of Computer Science, Aligarh Muslim University, Aligarh, India[4]

Abstract: Wireless Sensor Networks (WSNs) consists of tiny sensor nodes deployed in various geographic conditions to gather the information about the environment. The Intrusion Detection Architecture (IDA) in Wireless Sensor Network is used to detect various attacks occurring on sensor nodes of WSNs that are placed in various hostile environments. In the last few years, many innovative and efficient approaches have emerged in this area, and we mainly focus our attention on Trust based approaches of Intrusion Detection Architecture. In this article, our focal point of consideration is on Intrusion Detection Architecture for Wireless Sensor Networks. In addition, we present the security attacks and comparison of various Intrusion Detection Architectures.

Keywords: Wireless Sensor Networks (WSNs); Intrusion Detection Architecture (IDA); Security attacks; Types of Intrusion Detection.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are the collection of thousands of sensor nodes that are self-organized and are capable of communicating with each other wirelessly. But these nodes are constrained in terms of size, energy, memory, processing power [1]. These nodes sense environmental data, perform limited processing, and communicate over short distances. The applications of wireless sensor networks are continuously growing, and also the need for enforcing security mechanisms is increasing day by day. Wireless Sensor Networks may interact with sensitive data or usually these networks operate in hostile, unattended environments, it is necessary to address these security concerns and its related concept. Security challenges of sensor networks are different from traditional networks due to many constraints of these networks. Moreover, when we looked at the applications of WSNs, there are several applications areas, for example, battlefield awareness, traffic monitoring system, health environment etcetera in which security of information remains as an important issue [26]. Providing security to WSN is a nontrivial problem. Security mechanisms which are applicable to wired or other ad-hoc networks are not suitable for WSN. There are many reasons behind it, and we discuss those in the subsequent sections. Although, there are varieties of challenges in sensor networks [26], here we focused on different security issues and possible remedies of those.

Several papers have presented on the security attacks in WSN [2][25]. To deal with these attacks protection systems exist. Intrusion Detection Systems (IDSs) may be able to play an important role in detecting and preventing attacks. Furthermore, intrusion detection techniques must be designed to detect and prevent the execution of the most dangerous attacks. In addition, these techniques must be trust based to suit the limited resources of WSN. Energy consumption is a very important aspect in this type of network. Therefore, many researchers worked on this issue by proposing network architecture based on clustering approach [2][5][17]. This architecture consists of the creation of one or more cluster of nodes, and in each of them a cluster head is elected. This cluster head is accountable for collecting data sent by the members of his group, aggregation and subsequently transmitting data to the base station. This architecture is designed to minimize the power consumption of the nodes, and accordingly the extension of network lifetime.

This paper has been structured as follows: Section 2 gives an overview of security in WSN. Section 3 provides existing security attacks in WSN, while related work is discussed in Section 4. Brief introduction of IDA and its techniques is given in Section 5. It also describes the challenges in WSN, various types of IDS architectures followed by a comparison of IDS. Finally, we conclude the paper in Section 6.

----

[1] **Corresponding author:** Jeelani (email- jeelani.0018@gmail.com)

DOI 10.17148/IJARCCE.2018.71024

2. SECURITY REQUAREMENTS IN WSNs

The main security requirements that each Wireless Sensor Network has to fulfill are discussed below:

Data confidentiality: Secrecy of message transmitted between nodes should be maintained properly. For that important segments of message should be encrypted and in few cases even the two end points are also hidden. In some dynamic systems where nodes keep on joining and leaving the network, forward and backward secrecy needs to be maintained. Forward Secrecy means that nodes leaving the network may not be able to access future transmissions on the network after leaving the network and Backward Secrecy means that new nodes may not be able to access past transmissions before their joining the network. These phenomena are needed to maintain confidentiality of data in wireless sensor networks [6].
Authenticity: For ensuring the security of communicating nodes' identities, authenticity is very important. Any node should verify even if an accepted message comes from a true sender. In the absence of authentication, attackers without difficulty are able to extend wrong data into the WSNs. Generally, for authentication of the source of a message, an annexed message authentication code maybe employed.
Integrity: Integrity should be ensures to pledge that attackers cannot change the transmitted messages. Attackers are able to establish interference packets to modify their polarities. In addition before forwarding them a malicious routing node can modify important data in packets. To find random errors during packet transmissions, a cyclic redundancy checksum (CRC) is employed for detecting them, also keyed checksum, for example a MAC is used to secure packets against changes [1] [2].
Availability: WSN services should always be available in spite of all the resource depletion attacks that may occur on the system. Thus, a WSN network should be resistant to such attacks.
Non-repudiation: A transferred message has been sent or received by legitimate or authentic entity and they cannot deny.
Data freshness: Data freshness defines that no old messages have been replayed and that the data is recent. Especially, freshness of data is important for implementing shared key scheme.
Self-organization: This ensures that the each node should be self healing and self-organization in WSNs. But also self-organization is necessary to support multi-hop routing, and to conduct key management and building trust relations.
Auditing: The nodes of a sensor network must be able to store any specific events that occur inside the network. Sensor nodes are not directly operated by the users, but through the base station, therefore, users do not know about the existence of a certain event unless the nodes record it. Auditing information is used to analyze the behavior of the system in case of failure [5].

3. SECURITY ATTACKS IN WSNs

Since Wireless Sensor Networks operate in unsafe environment and hence these are vulnerable to several types of attacks.

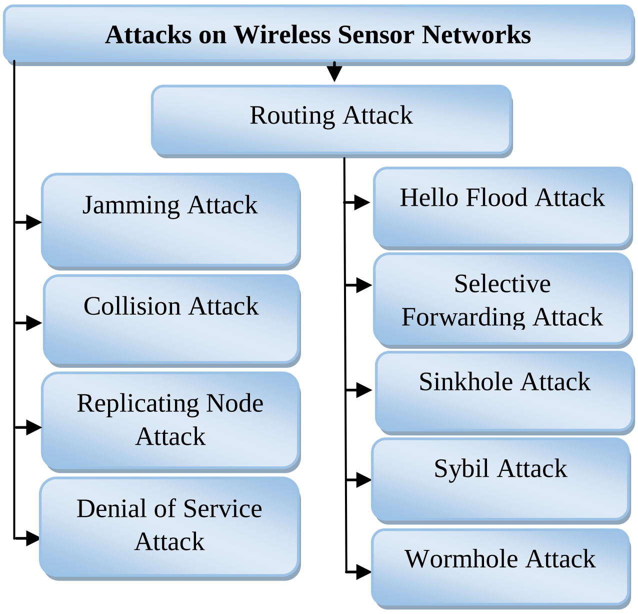

Figure: I Security Attacks in WSNs

DOI 10.17148/IJARCCE.2018.71024

Jamming Attack: Jamming Attack is caused by hampering the radio frequency of attacker nodes with the other nodes. This attack is accepted by the transmission of radio signals. It mainly causes the Denial of Service (DoS) attack and all the nodes are not communicating because of the jamming attack and mainly caused by jammer.

Collision Attack: In this collision attack, whenever the legitimate node is transmitting data, the attacker hears the transmission and transmits its own signal for producing interference. Even a collision of single byte can produce error and damage entire message. This collision attack is better than jamming attack with respect to consumption of power and detection ability. This attack intends at draining the communication channel and deprivation of network services [5].

Replicating Node Attack: The attacker may insert a new node into the sensor network which can be a clone node to a pre-existing node. This new clone node can transmit useful information to the attackers. The node replication attack is most dangerous when the cloned node is some base station. Hence, the base stations needs to be deployed in secure locations.

Denial of Service Attack: Denial of Service (DoS) attack is the serious attack as it consumes the network resources like energy, bandwidth and power. Denial of service attack floods access amount of unnecessary packets in the network and affects the overall performance of the network. If there is only single attacker in the network then this is called DoS attack. Moreover, if there are multiple attackers then this is known as Distributed Denial of Service (DDoS) attack. Denial of service attack is multilayer attack [2].

3.1. ROUTING ATTACKS

The attacks that affect the routing protocol of wireless sensor network are discussed below [25].

Hello Flood Attack: Hello Flood Attack is one of the active attacks that flood the hello packets in the network. In wireless sensor network attacker transmit the packets from source node to destination publicizing the packets as cluster head. All sensor nodes will select these packets and send join packet into it, thinking that the attacker is their neighbor and the entire network will be in confusion. In wireless sensor network the sensor nodes are deployed in normal orchestrated region. And the data is transmitted from source node to destination through intermediate nodes. Sensor nodes does not distinguish that the enemy node is not their neighbor node. So as a result network is spoofed by the attacker [2].

Selective Forwarding: In selective forwarding attacks, attackers can either drop packets randomly or selectively. It is much more challenging to defend these attacks than black-hole and on-off attacks. So this attack can be dangerous.

Sinkhole Attacks: Sinkhole Attack is to attract maximum traffic through malicious node which is placed somewhere near the base station. If the sensor network has one main base station then this attack can be dangerous.

Sybil Attack: In Sybil attack, one node presents multiple identities in the network that may mislead other nodes in the network. Sybil attacks can be used against topology maintenance and routing algorithms.

Wormhole Attack: Low latency connection between two parts of network over which an attacker replies network messages is a wormhole attack. This interconnection could be accepted by a single node sending messages between two adjacent non-neighboring nodes, or by a pair of nodes in uncommon parts of the network communicating with each other. The function of wormhole attack in network is exactly similar to sinkhole attack which attack node closing to base station [2][5][6].

Table: I Comparison of Attacks in WSNs

Attacks	Specialty	Impact	Defense
Sinkhole	Sinkhole Attack is to attract maximum traffic through malicious node which is placed somewhere nears the base station.	Lure away and to attract almost all the traffic; Triggering other attacks. Routing information or fake	Shortest path Drop the packets
Sybil	One node presents multiple identities in the network.	Fake and misleading message generated Resource exhaustion	Authentication, monitoring, redundancy
Selective Forward	The malicious node drops the packet and makes it unavailable to the destination.	intermediate node can detect abnormal packet loss and identify malicious nodes	Egress filtering, authentication, monitoring
Wormhole	The attacker sitting closer to base station may tunnel the traffic to a low-latency link thus disrupting the traffic.	Routing disruption disorder Fake/forged routing information confusion and WSN disruption	Offer less number of hops and less Delay which is fake
Hello Flood	It uses HELLO packets to persuade the WSN sensors.	Resources exhaustion; Confusion among nodes	Authentication

DOI 10.17148/IJARCCE.2018.71024

Collision	Internationally creating collisions in specific packets.	Interferences Data/ control exhausted confusion among nodes	Error-correction
Jamming	The frequency of attacker node is interfered with frequencies of stable nodes.	Collision of packets nodes resources exhausted confusion among nodes	Spread-Spectrum priority message lower duty cycle mode change

4. RELATED WORK

Ahmad, S. et al. [1] have concluded that networks require security plan due to various limitations of resources and the prominent characteristics of a Wireless Sensor Network (WSN) which is a considerable challenge in WSNs. The node nature causes limitations like limited energy, capability of processing, and storage capacity. These restrictions create WSNs so be distinctive from conventional ad hoc wireless networks [26].

Monika, B. et al. [2] have analyzed security issues and vulnerabilities in wireless sensor networks. All the security protocols mentioned should be using simulation and some more features like Speed-of- Operation, Power Consumption and Efficiency should be evaluated.

Wang, Q. et al. [3] have introduced a novel anomaly detection algorithm based security scheme. If each node can build a simple statistical model of its neighbor's behavior, these statistics can later be used to detect changes in them. They have shown that, by looking at a relatively small number of received packet features, a node can effectively identify an intruder impersonating a legitimate neighbor. The authors have considered that the anomaly detection algorithm be executed as each node separately.

Yuxin, M., [4] carried out the study to present a novel intrusion detection framework for WSNs. They tried to solve the problem of WSNs from a new point of view by using the multi-agent and semantic techniques. They introduced the layered architecture of the framework for WSN intrusion detection in detail. Further, they proposed several algorithms for intrusion detection based on the structure of WSN.

Shanthi, S. and Rajan, E.G., [5] discussed many potential issues of WSN security and detection mechanisms and presented a comprehensive analysis of various Intrusion Detection approaches (like, signature based detection system, anomaly based detection system, hybrid based detection system, etc) in Wireless Sensor Networks.

Usha, J. and Muzzammil, H., [6] have discussed challenges, security requirements, and different types of attacks. Comparing to the traditional networks; wireless sensor networks have limitations like low energy, storage capacity and computational capability, and security mechanisms and related work are also discussed.

Long, J. et al. [7] carried out the experimental study to develop a scheme for malicious node detection based on weighted-trust evaluation. A weight value was assigned to each sensor node initially. It updates every cycle if the node sends different report from the others.

Safiqul, I. M. et al. [8] have proposed an intrusion detection mechanism based on these existing approaches to identifying threats. WSNs offer a variety of prospective means to monitor environments. However, WSNs are vulnerable to various attacks for the reason that these networks are often deployed in open and insecure environments. Therefore, security design is an important feature of WSNs.

Eludiora, S. I. et.al [9] reviewed the existing approach for security solutions in WSNs and proposed the use of a distributed approach. This approach allows Sensor Nodes (SNs) to communicate directly with the base stations (BSs) rather than forming cluster-heads among themselves. Mobile Agents (MAs) were introduced to facilitate communication among the base stations (BSs). MAs can easily move from one host to another and perform necessary tasks. Researchers developed a Distributed IDS for WSNs. Distributed IDS is executing using TMote sky wireless sensor for testing and simulation over itemize parameters.

Fenye, B. et al. [10] proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects of trustworthiness, namely, social trust and QoS trust. Unlike prior work, they consider multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node.

Yanli, Y. et al. [11] presented a study by summarizing state-of-the-art trust mechanisms in two categories: secure routing and secure data. They firstly categorize all attacks related with trust schemes in WSNs, and use intelligent behavior attack to denote an inconsistent behavior attack in the content domain. Secondly, they analyzed the methodologies of trust schemes and emphasized the differences and challenges of trust schemes in WSNs.

Yassine, M. and Abedellah, E., [12] focused on intrusion detection systems (IDS), and examined existing approaches of Intrusion Detection in WSN. Authors have optimized security protocols for WSN. SPIN (Security Protocol for Information via Negotiation) has two security mechanisms: SNEP and TESLA. SNEP provides data confidentiality and data authentication while TESLA provides source authentication in multi cast scenarios by using MAC chaining. They are now working on their own model that incorporates all the advantages of the approaches proposed for a global model of intrusion detection in WSN.

Lamyaa, M. et al. [13] conducted the parametric study and proposed an integral mechanism which was Hybrid Intrusion Detection Approach based on anomaly, detection using support vector machine (SVM). Specifications based technique, Signature and clustering algorithm to decrease the consumption of resources, by reducing the amount of information forwarded. The aim was to establish a safe Wireless Sensor Networks without damaging the network, by the good management of resources specially the energy.

Hosein, M. and Arash, M., [14] have investigated security in Wireless Sensor Networks (WSNs) and presented a design process for achieving optimum security based on requirements and constraints in WSNs. WSN protocols focused on energy efficiency, transmission efficiency and routing. WSN is known for limitations on hardware and software and are resource constrained in general. An adaptive model of security that meets requirements and constraints in WSN is Intrusion Detections is discussed.

Yassine, M. and Abedellah, E., [15] have proposed a lightweight intrusion detection system for sensor networks, based on two existing models such as anomaly based and signature based. Indeed, the combination of these two techniques offers intrusion detection with a high detection rate. Intrusion detection model exploits advantage of support vector machine (SVM) and signature model to detect malicious behaviors and provide global lightweight IDS in cluster based topology.

Poongodi, M. and Bose, S., [16] have proposed a novel Intrusion Detection System. IDS are designed using the trust evaluation metrics, which is used for detection of flooding Distributed Denial of Service (DDOS) attacks in the network architecture. The proposed system combines the existing Firecol-based security procedures with Dynamically Growing Self-Organizing Tree Algorithm (DGSOT) in the trust evaluation-based environment. Researchers have used the simulator NS-2 for the evaluating the performance.

Alrajeh, N. A. et al. [17] have presented current Intrusion Detection Systems and some open research problems related to Wireless Sensor Networks security. Wireless Sensor Networks (WSNs) consist of sensor nodes deployed in a way to collect information about surrounding environment. Their distributed nature, multi hop data forwarding, and open wireless medium are the factors that create vulnerability to security attacks at various levels. Intrusion Detection Systems (IDSs) can play a main task in detecting and averting security attacks.

Wenjuan, L. et al. [18] carried out the experimental study to design an intrusion sensitivity-based trust management model that allows each Intrusion Detection System to evaluate the trustworthiness of others by considering their detection sensitivities, and further develop a supervised approach, which employs machine learning techniques to automatically allot the values of intrusion sensitivity based on expert knowledge. In the evaluation, authors compared the performance of three different supervised classifiers in assigning sensitivity values and investigate our trust model under different attack scenarios and in a real WSN.

Christiana, I. et al. [19] have proposed a general methodology of an anomaly-based Intrusion Detection System (IDS), named mIDS that uses the Binary Logistic Regression (BLR) statistical tool to classify local sensor activity to either benign or malicious to detect a malicious behavior within a sensor node. Attacks have been implemented within the Contiki O/S and tested the results using the associated COOJA simulator.

Mert, O. M. et al. [20] have proposed a novel hybrid IDS for clustered based WSNs by combining the “signature based approach” and “functional reputation based data aggregation and transmission method”. Instead of detecting the attacks only in the node level, they suggested a centralized and cooperative scheme using mutual trust evaluations between all network components.

Kumar, S. et al. [21] have investigated the impact of group mobility on performance of routing protocols under group mobility model using QualNet simulator. The researcher has illustrated that how the performance results of an ad hoc network protocol drastically change with the increasing node density. The various scenarios investigated with varying density of nodes in groups. Performance analysis is carried out on the basis of performance metrics under group mobility model and the DSR protocol clearly outperforms all other routing protocols with increasing node density under group mobility model. In case of WSN having mobile node, this study may be of great help in studying the behaviors of data communication among various nodes.

Abdulhamid, Z. and Faryad, P., [22] presented the parametric study to proposed a trust-based energy-aware routing algorithm. Considering direct and indirect trust of nodes and energy saving issue, the routing utility metrics are optimized by Gravitational Search Approach. This routing procedure is known as Energy-aware Trust-based Gravitational Search Approach (ETGSA).

Omkar, P. and Samita, P., [23] carried out the study on intrusion detection system (IDS) exploring the resources available as of today. Author also discussed the architecture of IDS in Wireless Sensor Networks based on their applications.

Anush, A. et al. [24] have reviewed various Intrusion Detection Systems (IDS) which can be broadly classified based on certain traditional techniques, namely signature based, anomaly based and hybrid based. The models proposed by several authors have been belittling verified based on certain classification parameters, such as detection rate, false alarm and algorithms. Authors have presented the summarization study of various intrusion detection systems that are used particularly in Wireless Sensor Networks, and also highlighted their distinct features.

DOI 10.17148/IJARCCE.2018.71024

Alquraishee, A.G.A. et al. [25] have analyzed the threats against the Wireless Sensor Networks, and proposed some possible measures to counter the attacks against the Wireless Sensor Networks.
Masood, S. and Zafar, A., [26] have discussed the distinctive features of WSNs which make routing in wireless ad hoc networks quite different from routing in their fixed counterpart. Researchers have iterated that Routing protocols for wireless sensor networks have to ensure reliable multi-hop communication and further described challenges in routing in wireless sensor ad hoc networks.

5. INTRUSION DETECTION SYSTEM

The threats, that spoil the security in WSN, can be detected by the Intrusion detection systems (IDSs). Intrusion Detection System attempts to identify computer system and network intrusions and misuse by gathering and analyzing data. The wireless Intrusion detection system can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity. Thus it is desirable to have several sensors that monitors the attacks and let each sensor report to a base station to avoid losing an important event. Security is a major concern in WSN due to its restricted resources like limited resources and vulnerable to physical attacks [25]. Some of the techniques used for security issues include key management, routing protocols, cryptography and security mechanisms for specific attacks and various IDS [5]. Intrusion Detection System has three main components [16] as shown in Figure II.

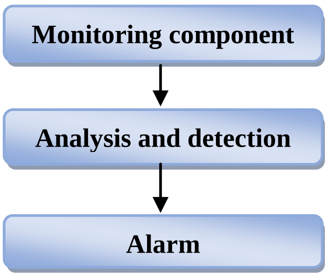

Figure: II Component of IDS

(i) Monitoring component is used for local events monitoring as well as neighbors monitoring. This component mostly monitors traffic patterns, internal events, and resource utilization.
(ii) Analysis and detection module is the main component which is based on modeling algorithm. Network operations, behavior, and activities are analyzed, and decisions are made to declare them as malicious or not.
(iii) Alarm component is a response generating component, which generates an alarm in case of detection of an intrusion.

5.1. CHALLENGES OF IDA IN WSNs

Some of the challenges involved in WSN are as follows [5] [6][26]:

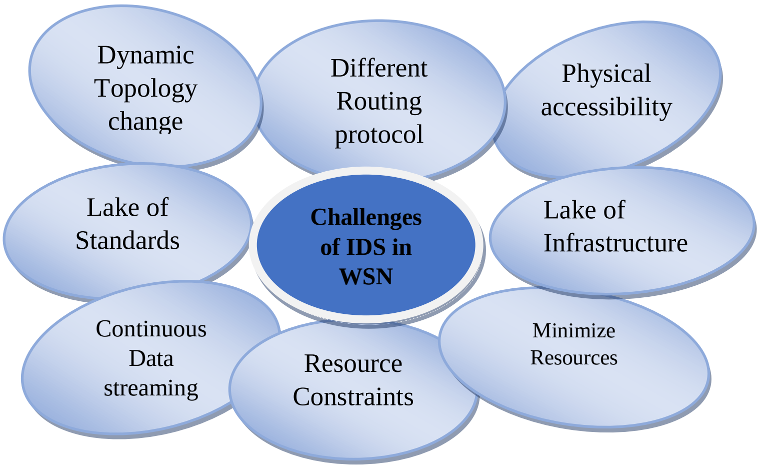

Figure: III Challenges of IDA in WSNs

5.2. INTRUSION DETECION ARCHITECTURES

Intrusion Detection Architectures are classified into two basic categories: host-based and network-based, depending on the data collection mechanism. Host-based IDS consult some types of log files (kernel, system, application, etc.) and

DOI 10.17148/IJARCCE.2018.71024

compare the logs against an internal database of general signatures for known attacks. Network-based IDS operate differently from host-based IDS. The design philosophy of a network based IDS are to scan network packets, auditing packet information, and logging any suspicious packets [5][17]. Additionally, IDS architectures can further be listed based on the detection technique. Signature based IDS centers on finding an amount of predefined signatures or behavior that matches a previously known malicious action or indicates an intrusion. The Anomaly-based IDS checks for any behaviors that fall outside the predefined or accepted model of behavior. The specification-based IDS defines a set of constrains that are indicative of a program's or protocol's correct operation. Various categories of IDS are discussed below.

Anomaly Based Detection System: This technique works on the basis of threshold; it compares the behavior of observed nodes with normal behavior. This model first describes normal behaviors which are established by automated training (as SVM) and then flags as intrusions any activities varying from these behaviors. It is able to detect new intrusions, but, it has a major disadvantage of missing out on well-known attacks. The anomaly based model has a high detection rate, but it has also a high false positive rate.

Signature Based Detection System: Misuse (Signature) detection based IDS have a predefined collection of main rules that is formed of previously known security attacks, so the behavior of nodes is compared with well-known attack patterns already existing in database. Although, this technique needs knowledge of attacks patterns and can't detect new attacks, so we always have to update attack signatures database.

Specification-Based Detection System: This technique is based on deviations from normal behaviors defined neither by machine learning techniques and nor by training data. Yet, specifications are defined manually and monitor any action by applying the predefined specifications.

Hybrid Based Detection System: This is organized of anomaly based along with signature based IDS system. It inherits the basic properties from anomaly based as well as signature based IDS system. One detection module verifies the known attacks using signatures and other module monitors the overall network behavior deviation from normal behavior. It is the most accurate detection system with less number of false positive. The major drawback of the hybrid system is to require more energy and resources. These IDS are mostly deployed in cluster based or to some extent in hierarchical WSNs; some are used to carry out signature based detection while others are used to perform anomaly detection in order to reduce the utilization of resources. Hybrid IDS are appropriate for large and sustainable Wireless Sensor Networks.

5.3. COMPARISON OF IDA

A comparison of popular IDAs in terms of various parameters like, memory utilization, energy consumption, detection rate and false alarm is presented in Table-II.

Table: II Comparison of IDA

Characteristics	Anomaly Based	Signature Based	Hybrid Based
Memory Utilization	Low	Low	Medium
Energy Consumption	Low	Low	Medium
Detection Rate	Medium	Medium	High
False Alarm	Medium	Medium	Low

6. CONCLUSION

In this paper, the survey of Intrusion Detection Architecture for Wireless Sensor Networks along with techniques used in various IDAs has been discussed. The various attacks and security of Wireless Sensor Networks have also being addressed in this study. The security in Wireless Sensor Network is very challenging and critical to the functionality of the network sensors. This becomes even more important in cases of highly secure environment, especially in industrial, military, and medical domains. The standard WSN protocols focus on energy efficiency; transmission efficiency, and routing. We observed from the previous studies that there is need of a new mechanism to protect the wireless networks from various attacks. However, traditional techniques are used to eliminate insider attacks up to some extent. In order to filter out compromised nodes from sensor networks, some trust-based systems have recently been modeled for Wireless Sensor Networks, which further needs to be strengthened in terms of security measures.

ACKNOWLEDGMENT

The authors are greatly indebted to the referee for his/her valuable comments and care reading of the manuscript.

DOI 10.17148/IJARCCE.2018.71024

REFERENCES

[1] Ahmad, S., Razzaque, M.A., Parisa, N. and Ali, F., "Security in Wireless Sensor Networks: Issues and Challenges", IEEE International Conference on Space Science and Communication (IconSpace), 2013, pp. 1-5.

[2] Monika, B., Nitin, P. and Brijesh, K., "Security Protocols for Wireless Sensor Networks", IEEE-International Conference on Green Computing and Internet of Things (ICGCIoT), 2013, pp. 1005-1009.

[3] Wang, Q., Wang, S. and Meng, Z. "Applying an Intrusion Detection Algorithm to Wireless Sensor Networks", IEEE-International Workshop on Knowledge Discovery and Data Mining, 2009, pp. 284-287.

[4] Yuxin, M., "A Semantic-based Intrusion Detection Framework for Wireless Sensor Network", IEEE- International Conference on Networked Computing, 2010, pp. 1-5.

[5] Shanthi, S. and Rajan, E.G., "Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks", International Conference on Next Generation Computing Technologies-IEEE, 2016, pp. 426-431.

[6] Usha, J. and Muzzammil, H., "Wireless Sensor Networks: Attacks and Countermeasures", International Conference on Advances in Internet of Things and Connected Technologies- Elsevier-ISSN: 1556-5068, 2018, pp. 584-590.

[7] Long, J., Hongjuan, L., Yaqiong, L., Weilian, X., Keqiu, L. and Zhongxian, C., "An Improved Intrusion Detection Scheme based on Weighted Trust Evaluation for Wireless Sensor Networks", IEEE-International Conference on Ubiquitous Information Technologies and Applications, 2010, pp. 1-6.

[8] Safiqul, M., Razib, K. H. and Bappy, D. M., "A Hierarchical Intrusion Detection System in Wireless Sensor Networks", International Journal of Computer Science and Network Security (IJCSNS), vol. 10 No. 8, 2010,pp. 21-26.

[9] Eludiora, S. I., Abiona, O.O., Oluwatope, A. O., Bello, S. A., Sanni, M.L., Ayanda, D. O., Onime, C.E., Adagunodo, E. R. and Kehinde, L.O., "A Distributed Intrusion Detection Scheme for Wireless Sensor Networks", IEEE International conference on Electro/Information Technology, 2011, pp. 1-5.

[10] Fenye, B., Ing-Ray, C., MoonJeong, C. and Jin-Hee, C., "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", IEEE Transactions on Network and Service Management (TNSM), Vol. 9, no. 2, 2012, pp. 169-183.

[11] Yanli, Y., Keqiu, L., Wanlei, Z. and Ping, L., "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", Elsevier-Journal of Network and Computer Applications, 2012, pp. 867-880.

[12] Yassine, M. and Abedellah, E., “A review of Security attacks and Intrusion Detection schemes in Wireless Sensor Network”, 2013, International Journal of Computer Science, pp. 1-12.

[13] Lamyaa, M., Hicham, B. and Mounir, R., "Implementation of a Hierarchical Hybrid Intrusion Detection Mechanism in Wireless Sensors Network", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, 10, 2017, pp. 270-278.

[14] Hosein, M. and Arash, M., "A Security Model for Wireless Sensor Networks", IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), DOI: 10.1109/CIVEMSA.2014.6841440, 2014, pp.1-6.

[15] Yassine, M. and Abedellah, E., "Lightweight Intrusion Detection Scheme for Wireless Sensor Networks", International Journal of Computer Science, (IJCS), 2015, pp. 1-8.

[16] Poongodi, M. and Bose, S., "A Novel Intrusion Detection System Based on Trust Evaluation to Defend Against DDoS Attack in MANET", Springer-Arabian Journal for Science and Engineering, vol. 40, Issue 12, 2015, pp. 3583–3594.

[17] Alrajeh, N. A., Khan, S. and Shams, B., "Intrusion Detection Systems in Wireless Sensor Networks: A Review", Hindawi-International Journal of Distributed Sensor Networks, DOI: 10.1155/2013/167575 2013, 2013 pp. 1-7.

[18] Wenjuan, L., Weizhi, M., Lam-For, K. and Horace, H. S. IP., "Enhancing Collaborative Intrusion Detection Networks against Insider Attacks Using Supervised Intrusion Sensitivity-Based Trust Management Model", Elsevier- Journal of Network and Computer Applications, 2016, pp. 1-15.

[19] Christiana, I., Vasos, V. and Charalampos, S., "An Intrusion Detection System for Wireless Sensor Networks", IEEE-International Conference on Telecommunications (ICT), 2017, pp. 1-5.

[20] Mert, O. M., Erdal, I. and Suat, O., "A Hybrid Trust Based Intrusion Detection System for Wireless Sensor Networks", IEEE-International Symposium on Networks, Computers and Communications, 2017, pp. 1-6.

[21] Kumar, S., Agrawal, G.S. and Sudhir, S. K., "Impact of Mobility on MANETs Routing Protocols Using Group Mobility Model", Wireless and Microwave Technologies, 2017, pp. 1-12.

[22] Abdulhamid, Z. and Faryad, P., "An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks", Springer-Peer-to-Peer Networking and Applications, 2018, pp. 1-10.

[23] Omkar, P. and Samita, P., "Application of IDS in WSN: A Survey", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol. 1, Issue 7, 2012, pp. 436-441.

[24] Anush, A., Tanmay, G. and Kunte, A., “Intrusion Detection System in Wireless Sensor Networks: A Review”, International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6, no. 12, 2015, pp. 131-139.

[25] Alquraishee, A.G.A., Zafar, A. and Hasan, S. H., “Security Issues in Wireless Sensor Networks”, Magnt Research Report, Vol.2(4), 2014, pp: 82-91.

[26] Masood, S. and Zafar, A., “Challenges in Routing in Wireless Sensor Ad hoc Network” in the proceedings of the National Conference NCCIST-2011, New Delhi, 2011.

DOI 10.17148/IJARCCE.2018.71024