Examination of Different Intrusion Detection System in Wireless Sensor Network Environment

L.Gandhimathi, G.Murugaboopathi

Abstract: ***In this era of emerging technology, Wireless Sensor Networks (WSN) has a huge number of Critical applications such as medical, smart grid monitoring the transformer, industries, etc. But Wireless Sensor Networks are susceptible to a large number of attacks due to its wireless nature. Security plays an important role for many real-world applications in WSNs. To develop secured WSNs, the intrusions should be detected before the attackers affect the sensor network. The modern surveys for different Intrusion Detection Systems (IDSs) in WSNs are considered in this paper. Initially, a general overview of flow-based IDSs is provided. Then, the survey reviews the related work on Cross-layer IDS and the applicability of those systems to WSNs. Then a brief survey is presented for Dynamic IDS. This is followed by trust-based IDS in WSN. Then, the survey reviews the related work on hybrid IDS in WSN. Finally, the survey for different ids in WSNs is analyzed. This paper highlights the open research issues in each of this field.***

Keywords: Networked sensors, Cross-layer IDS, Dynamic IDS, Hybrid IDS..

I. INTRODUCTION

IN Wireless Sensor Network, security plays an important role in many application areas, particularly for the military applications and healthcare applications. The sensor nodes are normally programmed to monitor or sense the Information from the nearest location and convey the sensed information to the base station.WSN node can be easily compromised because of its wireless nature. The attacker mainly focuses on the network layer, the physical layer, and the application layer.

Security plays a vital role in WSN. Providing Security to a sensor network need high memory capacity and high battery power is challenging. It is more challenging when we provide security using tiny sensor nodes. WSN has a great number of challenges based on the security. To protect the WSNs, intrusion detection systems (IDSs) are the best security mechanism. Moreover, greater security levels require more energy consumption in WSN. An IDS used for wired networks cannot be used for WSNs because of wireless nature, limited processing power, and low memory capacity. It is also difficult for the intrusion detection system to know the attacker motive, because the attacker behavior changes with respect to time.

WSNs are classified on the basis of the application and deployment scenarios. So the IDS designed for each sensor network may vary depending upon the applications.

Terrestrial WSN: Terrestrial WSN consists of sensor nodes deployed in the structured or unstructured pattern, on the ground.

Multimedia WSN: It consists of sensor nodes embedded with acoustic sensors, cameras or both. The major challenges in multimedia WSN are the processing and high bandwidth requirements.

Underwater WSN: In underwater WSN, sensor nodes are deployed on the seabed and along the ocean column. Autonomous Underwater Vehicles (AUVs) may be used for gathering data. The underwater sensor nodes use acoustic links to communicate with the surface station. Acoustic links have high latency; hence protocols developed for Radio Frequency (RF) based systems cannot be used without major modifications.

Underground WSN: Sensor nodes in underground WSNs are buried or deployed in the depth areas such as caves or mines. This method incurs a high cost for deployment and also for maintenance. Once deployed, accessibility will not be easy. The high attenuation and signal loss make the design of communication protocol in underground WSNs challenging.

Mobile WSN: In this category, the sensor nodes have the capability to move within the specified network areas.

The remainder of this paper is organization of article is as follows. The challenges in WSN are considered in section II. Types of security attacks are

Revised Manuscript Received on July 22, 2019.

***** Correspondence Author

L.Gandhimathi*, Computer Sceience and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email: lgandhimathi6@gmail.com

G.Murugaboopathi, *****, Computer Sceience and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email:gmurugaboopathi@gmail.com

presented in section III. Network Model and assumptions are considered in section IV. Section V presents taxonomy for the IDS Classification. Section VI concludes this paper.

II. CHALLENGES IN WSN

There are some technical challenges in WSN.

Ad hoc deployment:

In some cases, the sensors may be dropped from an air vehicle in the areas where human involvement is a difficult task (H. Wang X et al., 2007). In such cases, the sensors itself identify their positions and create a network connection with other nodes.

Unwatched operation: The large-scale deployments and the area of deployments make the network away from human involvement. In such cases, the sensors identify their positions and create a needed network. Otherwise, the energy of the node is wasted without doing any useful operations.

Untethered: The communication cost is high when compared to processing cost in WSN. Moreover, the nodes are also not connected to any power head. So, data transfer is minimized.

Network Failure: Network failures can occur due to many reasons such as the failure of a node, irregular radio connectivity, link failure and so on. Node failures occur due to many reasons such as component failure, node destruction by an external event, or when a sudden battery level depletion occurs. Network partition occurs due to link failure.

Dynamic changes: Failure of nodes and addition of extra nodes occurs in WSN. So, the connectivity should be maintained at every point of time.

Basic requirements in WSNs

- Low Power Consumption
- Highly secure
- Ease of use
- Scalability
- Responsiveness
- Bi-Directional Communication
- Reliability

Basically, WSNs suffered from various types of attacks, including Sybil attacks, Wormhole attack, DOS attack, selective forwarding attacks, and sinkhole attack. Because of its transmission medium and its deployment in the open environment, it is very difficult for solving all security issues by using prevention method alone.

So the detection method plays an important role. The intruder should be detected before it affects the environment. Some examples of intrusion are:

- Guessing and cracking credit card numbers
- Tunnelling the valuable information to the attacker

The most important step in efficient WSN design is to optimally place the sensor nodes in order to meet the desire coverage and connectivity.

III.TYPES OF SECURITY ATTACKS IN WSN

Generally, sensor network s attack can be categorized into the following:

Active versus passive attacks: Active attack involves doing some alterations in the information stream, where as passive attacks involve just eavesdropping the packets traded within a network.

Outsider versus insider attacks: Outsider attacks are threats that create an attack from nodes that are outside of the WSN. Insider attacks happen when genuine nodes do some unauthorized activity in WSN.

Mote class versus laptop-class attacks: In former case, an adversary damages the functionality of a WSN by making use of a few nodes having similar abilities. In later-case, the attacker can make use of more powerful devices such as a laptop to attack a WSN.

Hansman and Hunt (2005) proposed first dimension of the attack taxonomy

Some of the following types of attacks are

Table 1: Attack Types

Category	Subcategories
Viruses	Boot sector virus Web scripting virus
Worms	Email Worms Internet Worms
Buffer overflows	Stack based Heap based
DoS attacks	UDP Flood IP Fragmentation attack HTTP Flood
Network attacks	Browse hijacker Malware Attacks Web attacks
Password attacks	Brute force Key loggers

Denial of Service (DOS) attack – Here, any type of intentional activity that can destroy the network resources and also will not allow the legitimate user to access the resources.

Clone attack – The clone attack also known as node replication attack. Here, the attacker copies the cryptographic information of another node.

Sinkhole attack – In this attack, an attacker forges the routing information to their neighboring nodes, which look more attractive in the network.

Sybil attack – Here a single node presented itself to many nodes with multiple spoofed identifications of any network or MAC addresses.

Wormhole attack – The wormhole attack involved in more than one malicious node. The attacker receives data packets from one location to another location through the tunnel known as wormhole link. Once the wormhole link is established, an attacker captures the wireless transmission through the wormhole link.

Flooding attack – Generally, this attack generated a large volume of traffic, which prevents the valid user from accessing services.

Tampering attack – In this attack, an attacker extracts the sensitive information like keys or password etc.

Man in the middle attack – It is an eavesdropping attack in which an attacker establishes an independent connection between the nodes with victims.

Eavesdropping attack – In Eavesdropping, the attacker secretly overhears confidential information in an unauthorized way in private network.

Selective forwarding attack –In this, the attacker, selectively dropped the data packets coming from a group of nodes or particular node. Another name for this attack is grayhole attack.

The main intention of this work has to provide more security for WSN by analyzing the issues present in the network. The main aim of the IDS is to identify the attackers. In some case, if every sensor takes part in the detection operation then intrusion detection process is not energy efficient. To operate IDS in a successful way for a long duration of time, energy saving is needed and this can be achieved by using dynamic management. Dynamic management minimize the energy drain for the sensor networks by making some set of nodes is active while another set is allowing them to sleep. In this case, some nodes are scheduled to wake up while the remaining nodes are put in the sleep state.

Some of the detection techniques focus on known attacks while the other detection techniques focus on unknown attacks. Known and unknown attacks are easily identified by signature based and anomaly-based intrusion detection system respectively. In some case, even if an attacker is not able to find an attack, he may be able to get some new capabilities from the attack.

A hierarchical based intrusion detection system may involve three levels of detection. Initially node level detection, followed by cluster-level detection, and then sink-level detection. In node-level detection, the nodes are responsible for the detection process. Here, individual node periodically samples the event and sends to the particular cluster head. In Cluster-level detection, the cluster head is responsible for the detection process and collaborative data is maintained for the detection process. In order to improve the detection performance and decrease the false positive rate by cooperatively detect an attack using multiple nodes. In sink-level detection, the base station is responsible for the detection process. The spatial and temporal correlation can be used to improve the reliability of detection process. Intrusion detection in wireless sensor network consumes high energy for the detection process. In addition to that, we can select the intrusion detection features from network characteristics such as number of packet send, number of packed received and dropping ratio of nodes, energy level, the routing information, type of the packet, the energy needed, and packet length.

Many intrusion detection systems are available in the market, but choosing the best intrusion detection system for an organization is a difficult task. The best intrusion detection system will be chosen based on the detection rate. The Detection rate can be calculated using the following formula

$$Detection\ rate = \frac{Detected\ Attack}{Total\ No\ of\ Attack} * 100$$

It is very important to locate the position of the sensor node. In general, Intrusion detection techniques can be categorized into different ways: misuse based, anomaly-based, and trust-based. Combination of signature-based detection techniques and anomaly- based detection techniques achieve more detection rates and less false positive rate.

Snort is an open-source IDS where its databases are freely accessible and maintained by online. Snort has rules for the header as well as to the packet payload that allows the analysis to be carried out. Based on the predefined rules the packets are filtered. Snort is one of the light-weight NIDS.

IV. NETWORK MODELS AND ASSUMPTIONS

A.BASED ON STATES WITH TRANSITIONS

The nodes in Sensor Networks are classified into

three states based on energy consumption. They are ideal, monitoring and active states. In the ideal state the nodes are in sleeping stage and there is less energy consumption, whereas in the monitoring state consume more energy than ideal state because the nodes observe the activities of other node and delivering the data to the destination at a regular interval of time. The highest energy is consumed by active state when compared to ideal and monitoring states, because huge amount of data are transmitted in active state.

B. TYPES OF DATA TRANSMISSION TO SINK

The sensed data of a nodes transmitted to the sink node can be classified into four types. They are continuous model, request-reply, event-driven model, and edge-trigger model. In continuous model, the sensors node delivers the sensed data continuously at a pre-defined rate. In the event-driven model, the sensed data are delivered immediately to the sink, when abnormal or irregular events happen in the network. Edge-trigger model observes the data and informs to the base station when it crosses the edges or boundary. In request-reply model, based on sink requirement the sensor node reply to sink.

C. INTRUDER BEHAVIOUR PATTERNS

One of the behaviors of the intruders is the continuous shifting of their states. The attack that originated from outside the organization is known as intrusions while the attack that occurs inside the organization known as misuse.

The main aim of the malicious node is to break the functionality of WSN. Based on an assumption the malicious node can perform the following attacks:

Packet dropping attacks: In this, the malicious node can drop the packets while forwarding the packets to the base station.

Data modification attacks: The attacker can perform some modification on the data to corrupt the data packet.

D. PERFORMANCE EVALUATION CRITERIA

True positive (TP): This represents the number of normal records that are correctly classified.

True negative (TN): Here the number of abnormal records that are correctly classified.

False positive (FP): False positive incorrectly predicted the normal activities as abnormal.

False negative (FN): In this the events are not marked as intruder by the detection method even though the attack exists.

The accuracy can be calculated using the following formula:

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN}$$

Table 2: Confusion matrix

Actual value	Predicted value	
	Normal(+)	Abnormal(-)
Normal(+)	True Positive	False Negative
Abnormal(-)	False Positive	True Negative

There are two important terms that need to be considered in intrusion detection systems – false positives and false negatives.

The false positive indicates normal nodes recognized as malicious nodes (MN). The false positive rate is defined as the percentage of nodes incorrectly detected as malicious node, when the node is not malicious.

$$\textbf{False positive rate} = \frac{\text{No of Normal node recognized as MN}}{\text{No of Whole normal nodes}}$$

The false negative malicious nodes is recognized as normal nodes, and the false negative rate is defined as the percentage of malicious nodes recognized as normal nodes to the total number of malicious nodes.

$$\textbf{False negative rate} = \frac{\text{No of MN recognized as normal node}}{\text{Total number of malicious node}}$$

For the best intrusion detection system, we need to reduce the false positive rate as well as false negative rate.

V. IDS CLASSIFICATIONS

The IDS is classified based on the layers of OSI model, mobility, flow based, Trust model and hybrid model. Different ids classification is shown in fig.1

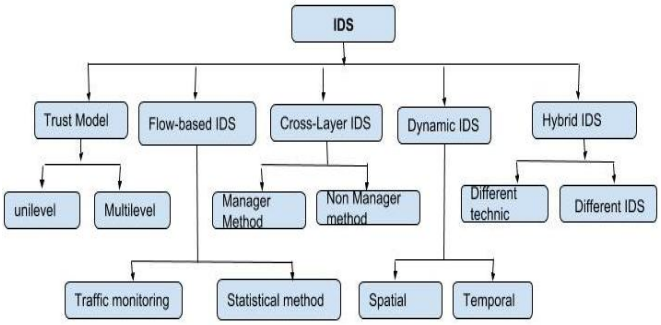

Fig.1.IDS classifications

ACTIVE-BASED AND PASSIVE-BASED IDS

Active IDS are otherwise known as an intrusion prevention system — the configuration of IPS is designed in such a way that automatically block suspected attack in advance without using any human intervention. A passive IDS is configured in such a way that monitor analyzes network traffic activity and alert only if it detects an attack.

HOST-BASED IDS AND NETWORK-BASED IDS

The host-based IDS examine the activities of the particular host on which it is installed. It also collects and analyzes information on the host system.

Drawbacks of HIDS

- HIDS disables the IDS after the system is compromised.
- It is difficult to analyze the intrusion on internet computer.

Network-Based IDS: It has a network sensor with a Network Interface Card (NIC). Network-based IDS operate on the network level and analyze the network traffic.

KNOWLEDGE-BASED AND BEHAVIOUR-BASED IDS

A Knowledge-based IDS references the previous known attack profiles database to identify an attack. A behavior based IDS make a reference with baseline profile of normal activities to identify an attack. Deviations from this baseline profile generate an alarm. Node deployment plays an immense role in intrusion detection. Heterogeneous WSNs comprise sensor nodes with dissimilar computing power and sensing range.

Based on the types of node deployment, the WSN can be classified into different types

The types of nodes are:

- Static or moving.
- Known location or unknown location.
- Sensors of homogenous or heterogeneous.

Based on the number of sensors participated in the deployment process, the sensor network problem will be considered.

- Sensor problems with one sensor

The problem in one sensor is due to node death caused by power battery discharge (Szewczyk et al., 2004).

- Link problems in between two sensors

The problem in two sensors is link failure or network congestion due to huge traffic bursts (Szewcyk Mainwaring et al., 2004), and also the presence of asymmetric links.

- Path problems more than three sensors

The different path leads routing loops and also weak path to sink will create such kind of failures.

- Based on Layers and Mobility of IDS

In addition to the above classification technique, IDS can be classified based on the layers used for detection purpose and also deals with the mobility of the nodes used for the detection process.

Flow-Based IDS

Based on traffic monitoring and statistical methods the attacks are analyzed. Fabrizio Angiulli, et al [1] proposes intrusion detection technique for monitor the application traffic and raising alerts when intrusions are identified. In flow-based intrusion detection system inspects only the packet header without checking the payload of the packet and IP flow records. So the attack hidden in packet payload cannot be identified using flow-based intrusion detection systems. Here IP flow records are given as input and it checks whether the flow of traffic is normal or misbehavior. (Sperotto and Pras, 2011). Muhammad Fahad Umer et al [7] proposes two-stages of flow-based intrusion detection model. The first stage separates malicious flows from normal flow in the network. But it cannot detect specific type of attack using malicious flows. So, these malicious flows need a human intervention to detect the specific type of attack and corrective actions during the second stage. John a Clark et al [8] propose the deployment problem of IDS in WSN. Three basic issues to be considered in placing IDS first placement configuration problem next total attackers finally resources consumption. IDS are placed in areas where more amounts of attackers can be easily found out without wasting energy resources. Identical IDS is placed, each IDS is responsible for the particular attack. Activation and deactivation of IDS in the network is user dependent. Placement configuration problem is taken as a major factor (issue) and various algorithms like local search

algorithm are being proposed to find an optimal solution for the practical application. This analysis is general and it is applicable to any WSN. Amin Hassanzadeh, et al [9], proposed to decentralize the architecture. A solution in which a base station has knowledge about network and security requirement of all nodes, the node which does intrusion detection is denoted as monitor nodes, or co-operators or aggregators or cluster head. The network is organized as a set of cluster tree and each running is distributed as local IDS. D.K.Singh, et al [10], proposed the hierarchical network model. Each cluster head is responsible for monitoring its members. The CH collects information from all its member node. Yating Wang, et al [11] proposes an intrusion detection using the code attestation technique for detecting the attacker node. Energy consumption is high when the code attestation happens frequently. If the code attestation is not done frequent, then attacker may not detect an attack in time. Guorui Li, Jingsha He, Yingfang Fu[12], propose a distributed group-based intrusion detection scheme that meet all the requirements such as efficient, lightweight and flexible intrusion detection algorithm. Here the sensor network is partitioned into many groups and each group is physically closed to each other group and all groups have the same sensing capability. In Group-based intrusion detection, the sensor nodes are grouped and running the group based intrusion detection algorithm in each group. The sensor nodes which are spatially close to each other has the similar behavior. If some sensor node finds different behavior in the same group, that node will be isolate from the group in order to keep the secure network.

Cross-Layer IDS

The existing Intrusion detection system focuses on single layer of WSN without considering other layers. For example, the network layer agent can detect few types of attacks in that particular layer only (e.g., routing attacks like sinkhole attack, Sybil attack) and will not detect an attacks coming from other layers such as Physical layer (e.g., Jamming attack). But, the cross-layer IDS have the capability to detect most of the attacks coming from different layers in the OSI model. Also, the performance of the overall architecture of a standardized layer protocol stacks is limited, due to lack of coordination among layers. The cross-layer design should maintain the functionalities of traditional layer but it will allow the layers to coordinate with each other to perform joint optimization of protocols across different layers. There is a close cooperation between the layers which lead to the optimization of the cross-layer functionalities. Based on the sharing of information the cross-layer structure can be classified into two types. They are manager method and non-manager method. In manger method, function of the protocol is changed, but does not change structure of TCP/IP model. It shares the data with some or all of the layers. In the non-manager method, any two layers can be communicated directly. Boubiche and Bellamy [13] proposed IDS system maintained the traditional layered architecture using an agent for communication in Cross-Layer Intrusion Detection. The main advantage of this method included a free access to all the layers and decision making was more efficient when compared to a single layer Williams Horton [14] proposed an algorithm in this each protocol layer perform the function to improve the intrusion detection performance using bio-inspired evolutionary approach. John Felix Charles Joseph, et al, [23] proposes a method with reduced feature set and high detection accuracy by correlating one or more features from different layers to a particular MAC layer feature. Lucas D.P Mendes, et al [16] provided the solution to the challenges faced by the WSN applications using cross-layer approach. The optimization techniques used in this approach have been proven as an efficient method to solve the problem faced by WSN. L.Gandhimathi et al [15] proposed intrusion detection by correlating cross layer features and using mobile agent to detect multiple attacks in WSNs.

Dynamic IDS

The existing researches have focused mainly on the stationary sink as well as stationary node based WSN. So, the intruder across the region is to be detected easily by the intrusion detection techniques. But recently most of the real-time applications are based on the mobile sink and mobile nodes. So, the existing detection techniques are not suitable for dynamic networks. Applying IDS for mobile nodes or dynamic change of network environment with respect to topology is a challenging task. Spatial correlation and temporal correlation can be used to identify mobile intruder, based on change of location and time interval. So, auto-configurability and scalability of IDS should be applied for dynamic change of network topology. Introducing mobility in WSN helps to improve connectivity, coverage, reliability, reduction in deployment cost, energy efficiency, etc. Mobile WSN is used to improve the QOS of the existing terrestrial WSN. The motive of dynamic IDS is to improve the performance of existing terrestrial network using mobile sensor nodes. Mobile nodes can relocate the position for improving the connectivity and coverage of WSN. The energy consumption can be reduced in the sensor network by using mobile node.

The ongoing communications are affected in dynamic topology due to frequent link failure. In a static sensor network, the node position is fixed while in a mobile node, the location information needs to be frequently updated. Mobile WSN needs frequent neighbor discovery and fast

localization; hence the amount of control overhead is high, as compared to static WSNs. Even though the time critical application such as event monitoring application, the need for sensing the entire area with stationary nodes may not be efficient and economical. If we make all the node as in dynamic nature then the interference is high. So, the alternate way is to monitor the area with several static sensors and few mobile sensors that can collaborate in order to improve the network performance to detect or to perform certain action as fast as possible. Michael Riecker, et al [5] proposed a lightweight, energy efficient system, which makes the system in energy efficient way, by using the mobile agent to detect intrusion with less energy consumption of the sensor node. Sina Hamedheidari, et al [6] proposed new approach based on mobile agents. Here the mobile agent has to inform the message only to the valid nodes. So that the valid node will not listen the traffics generated by malicious nodes. By this way, the sinkhole attacks can be detected using mobile agents. Jiming Chen et al [17] have proposed the Mobile target detection method and also develop the theory of circle graph method for a significant application in WSNs. Jun-Won Ho, et al [18], in their paper; the authors proposed a technique called Distributed Sequential Probability Ratio Test (SPRT) method to detect the mobile malicious node in static sensor network. Nodes in sensor networks are fixed in their position after deployment. However, an attacker who compromised some set of nodes need not be in the same location all the time. The attacker may move his compromised nodes to multiple locations in the network. The source of attacks can be easily found by this method.

Hybrid IDS

Hybrid IDS combines misuse IDS and anomaly-based IDS. In order to improve the performance the hybrid ids combines different technique or different ids. The hybrid optimization technique is proposed for both deployment and routing of nodes in wireless sensor networks. Also this technique uses the fuzzy logic concept for determining the position of each nodes and it uses the particle swarm optimization technique to deploy and route the nodes in the bounded region. The objectives are: a) To deploy and route the nodes b) To avoid the collision in wireless sensor networks c) To activate Asynchronous Sleep and Wake-up Procedure. The main advantage of the hybrid optimization technique increases the network coverage faster than the other algorithm.

Safa Otoum, et al [3] has proposed hybrid architecture to detect both the unknown and known attacks. Here the unknown attacks are detected by anomaly detection method such as Enhanced Density –Based spatial clustering of application with noise whereas the known attacks are detected by the signature detection method such as Random Forest methods. Ziwen Sun, Yimin Xu, et al[2] proposed the V-detector algorithm for Wireless Sensor Networks (WSN) for the best intrusion detection using memory detector set and mature detector set are the two kinds of detector used to detect the intruder effectively and reduction in data storage space and computation cost. Chenghua Tang, et al, [4] proposed hierarchy based anomaly intrusion detection model here the genetic algorithm based fuzzy c-means with the SVM method to improve the effectiveness of intrusion detection system.

Trust-Based IDS

Trust management can be applied in WSNs to reduce the power of the compromised sensor node that injects malicious data in the sensor network. Trust-based IDS can be classified into two types. They are single level trust and multilevel trust. Raja Waseem Anwar, et al [19] proposed new protocol known as Trust Aware Wireless Routing Protocol (TAWRP).Here the optimal routes are established with trusted node for minimize the packet loss while forwarding the packet to the destination and isolate the malicious node from the network. According to Mohsen Salehi , et al[20], each node calculates the trust values of neighbour node initially and according to these values the data are exchanged with its neighbour nodes, then from each cluster, a node whose trust is greater than a threshold value can be selected as cluster members. Then using the fuzzy logic a node with the most trusted neighbors and desirable energy level is designated as a cluster head. The proposed system greatly improves security and prevents trustless and malicious nodes from becoming the cluster head. Zhi Hu, et al [21] analyzed the attacks and designed the dynamic time window for the distributed trust model with the detection of direct trust and indirect trust. Here, only trusted nodes are considered and constructed the trusted tree, which is based on the path quality of nodes which is used as the gradient for routing.

Table 3: Comparative analysis of different IDS

IDS Types	Technique	Description	Advantages	Disadvantages
Flow-Based IDS	One class-SVM based model[1]	Flow-based intrusion detection systems, analyze the flow of traffic as normal or abnormal, based on IP flow records.	It only inspects the packet header. so time taken is less	Flow-based techniques Consider only the packet header and Not able to detect the attacks hidden in the packet payload cannot be detected and the accuracy is less when compared to packet-based detection.
Cross-layer IDS	Bio-inspired evolutionary computational method [16] Low Energy Self-Organising Protocol(LESOP) [22]	Intrusion detection performances are improved using the embedded function, genetic algorithm and ant colony optimization and trust-based model. Here the interaction between the Application layer and MAC layer are directly exploited.	Improves overall IDS performance instead of assigning detection performance in only one layer's function. In order to simplify the protocol stack the few layers are excluded in LESOP	Extra overhead by considering and collecting information from different layers using bio-inspired method. The performance of the overall architecture of a standardized layer protocol stacks is limited, due to lack of coordination among layers.
Dynamic IDS	Distributed Sequential Probability Ratio Test (SPRT) scheme [18]	If the attacker moves his compromised nodes to several locations in the network, he can escape from the location where the source of attacks is created.	Able to detect the mobile malicious node using this SPRT scheme.	Detection processes are done locally.
Trust-based IDS	Trust Aware Wireless Routing Protocol (TAWRP) scheme[19]	In TAWRP, optimal path is established using trusted nodes and effectively forwards the packet from source to destination.	TAWR achieved high packet delivery ratio when compared to other trust based protocol.	Routing overhead is high when the number of malicious nodes increases.
Hybrid-IDS	Random Forest (RF) methods and Enhanced Density-Based Spatial Clustering of Applications with Noise (E-DBSCAN) [3]	Hybrid architecture to detect both the unknown and known attacks.	RF and E-DBSCAN method has a high possibility to detect both known and unknown attacks	This method is time consuming process, because of checks anomalies behavior and also analyzes the signatures pattern.

VI CONCLUSION

Major threat for WSN is the injection of malicious data. The detection techniques are identified in five main aspects. First aspect based on flow based IDS. Here the flow of traffic is analyzed based on IP address of packet header and consider it as normal or malicious. Next aspect is based on cross layer IDS. Only adjacent layers are communicated in standard TCP/IP model. But, in cross-layer designs the information is shared with all the layers. Techniques can be performed more optimally by using cross-layer design, rather than using a fixed TCP/IP model. Then the third aspect is based on Dynamic IDS. The solution for mobile malicious node is considered and the intrusion detection technique with respect to dynamic environments was presented in this paper. The next aspect is based on trust-based IDS. Here the trust management technique is applied in sensor network to reduce the number of malicious nodes. Finally, the hybrid IDS is designed using both anomaly detection method and misuse detection method. Then it is analyzed and compared with different aspects of IDS model. Across all the aspects, the excellent model of IDS is designed to satisfy the expected behavior.

REFERENCES

[1] Fabrizio Angiulli, Luciano Argento, and Angelo Furfaro, "Exploiting Content Spatial Distribution to Improve Detection of Intrusions", ACM Transactions on Internet Technology 2018; **18**(2):1802-1825

[2] Ziwen Sun, Yimin Xu, Guangwei Laing and Zhiping Zhou "An Intrusion Detection Model for Wireless Sensor Networks with an Improved V-detector Algorithm", IEEE SENSORS JOURNAL 2018; **18(**5): 1971-1984.

[3]Safa Otoum, Burak Kantarchi, Hussein T.Muoftah, "Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications" IEEE SENSORS LETTERS 2017; 2(3): 1-4.

[4] Chenghua Tang, Yang Xiang, Yu wang, Junyan Qian, Baohua Qiang", "Detection and classification of anomaly intrusion using hierarchy clustering and SVM", Security and Communication networks 2016;**9(**16):3401-3411.

[5] Michael Riecker , Sebastian Biedermann, Rachid El Bansarkhani, and Matthias Hollick, "Lightweight energy consumption-based intrusion detection system for wireless sensor networks" international journal of information security 2015;**14(**2):.155-167.

[6] Sina Hamedheidari, Reza Rafeh, "A novel agent-based approach to detect sinkhole attacks in wireless sensor networks", Elsevier Journal of computer and security 2013; **37**:1-14.

[7] Muhammad Fahad Umer, Sher M Bi Y**, "**A two-stage flow-based intrusion detection model for next-generation networks" Plos one, 2018; **13**(1) 10.6084/m9.figshare.5756520

[8]Juan E.Tapiador, John A. Clark "The placement-configuration problem for intrusion detection nodes in wireless sensor networks", Computers and Electrical Engineering 2013; **39(**7): 2306–2317.

[9] Amin Hassanzadeh, Radu Stoleru," On the Optimality of cooperative intrusion detection for resource-constrained wireless networks, Computers, and Security, 2013; **34**, 16 -35, 10.1016/j.cose.2013.01.002

[10].Shun-Sheng Wang, Kuo-Qin Yan, Shu-ching Wang, Chia-Wei Liu," Intrusion detection based security solution for cluster-based wireless sensor networks, an Expert system with applications 2011; **38**:15234-15243.

[11].Ing-Ray Chen, Yating Wang, Ding-Chau Wang **"**Reliability of wireless sensors with code attention for intrusion detection", Information Processing Letters 2010; **110**(17):778–786.

[12]. Guorui Li, Jingsha He, Yingfang Fu, Group-based intrusion detection system in wireless sensor networks, Computer Communications 2008; **31**(4):4324–4332.

[13] Boucher and Bellamy," Cross-layer intrusion detection for wireless sensor network "International Journal of Network Security & Its Applications 2012; **4**(2):34-52.

[14] William S.Hortos, "Bio-Inspired, Cross-Layer Protocol Design for Intrusion Detection and identification in Wireless Sensor Networks "IEEE workshop on security in Communication Networks 2012;1030-1037.

[15] L.Gandhimathi and G.Murugaboopathi," Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent", International Conference on communication and Embedded Systems, 2016, DoI: 10.1109/ICICES.2016.7518935.

[16]Lucas D.P Mendes, et al, "A survey on cross-layer solutions for wireless sensor network", Journal of Network and computer Applications, 2011; **34**(2):523-534.

[17] Jiming Chen, Junkun Li, and Ten H.Lai, "Trapping Mobile Targets in Wireless Sensor Networks: An Energy-Efficient Perspective" IEEE Transactions on Vehicular Technology 2013; **62**(7):3287-3300.

[18]Jun-Won Ho, "Distributed detection of mobile malicious node attacks in wireless sensor networks", Elsevier journal in Adhoc Networks 2012; **10**(3): 512-523.

[19] Raja waseem anwar, Majid Bakhtiari, Anazida Zainal and kashif Naseer Qureshi "Malicious node detection through trust aware routing in wireless sensor networks", Journal of Theoretical and Applied Information Technology 2017; **74**(1):88-92.

[20] Mohsen Salehi, Jamal Karimian, "A Trust-Based Security Approach in Hierarchical Wireless Sensor Networks", International Journal of Wireless and Microwave Technologies 2017; **6**: 58-67.

[21] Zhi Hu, et al, "Trusted Tree-Based Trust Management Scheme for Secure Routing in Wireless Sensor Networks", International Journal of Distributed Sensor Networks 2015; **11**(12):1-13.

[22]Liang Song, Dimitrios Hatzinakos, "Cross-layer architecture of wireless sensor networks for target tracking", IEEE transaction on Networking 2007;**15**(1):145-158.

[23] John Felix Charles Joseph et al, " Cross-Layer Detection of sinking behavior in Wireless AdhocNetworks using SVM and FDA", in IEEE Transactions on Dependable and Secure Computing 2011; **8**(2):233-245.

AUTHORS PROFILE

L.Gandhimathi holds M.E. in Computer Science and Engineering from Anna University, Chennai, India, 2008. She is pursuing her Ph.D. degree in the area of Wireless Sensor Networks. Presently she is a Research Scholar in department of Computer Science and Engineering, Kalasalingam academy of Research and Education, Krishnankoil, India. Her areas of interest include wireless sensor networks, data structure and algorithms, Compiler Design, and Network Security.

G.Murugaboopathi received the Undergraduate Degree in Computer Science and Engineering from Madurai Kamaraj University in 2000, the Post Graduate degree in Digital Communication and Network from Madurai Kamaraj University in 2002 and Ph.D in Computer Science and Engineering at Bharath University, Chennai. He has more than 45 Publications in National, International Conference and International Journal proceedings. He has more than 15 years of teaching experience. His areas of interest include Wireless Sensor Networks, Bioinformatics, Mobile Communication, Mobile Adhoc Networks, Mobile Computing, Cloud Computing, Network Security, Network and Data Security, Cryptography and Network security. He is currently working as an Associate professor in the Department of Computer science and Engineering at Kalasalingam Academy of Research and Education, Tamil Nadu, India..