A Study on Intrusion Detection System in Wireless Sensor Networks

Sravanthi Godala[1], Rama Prasad V. Vaddella[2]

[1]JNTUA, Ananthapuramu (AP), India
[2]Sree Vidyanikethan Engineering College (Autonomous), Tirupati (AP), India

Abstract: The technology of Wireless Sensor Networks (WSNs) has become most significant in present day. WSNs are extensively used in applications like military, industry, health, smart homes and smart cities. All the applications of WSN require secure communication between the sensor nodes and the base station. Adversary compromises at the sensor nodes to introduce different attacks into WSN. Hence, suitable Intrusion Detection System (IDS) is essential in WSN to defend against the security attack. IDS approaches for WSN are classified based on the mechanism used to detect the attacks. In this paper, we present the taxonomy of security attacks, different IDS mechanisms for detecting attacks and performance metrics used to assess the IDS algorithm for WSNs. Future research directions on IDS in WSN are also discussed.

Keywords: Intrusion Detection, IDS mechanisms, Performance metrics, Precision-Recall curve, Receiver operating curves, Security attacks, Wireless Sensor Networks

1. Introduction

Wireless Sensor Network (WSN) is a background technology for the Internet of Things (IoT) and investment on WSN was $0.45 billion in 2012. It is estimated to increase $2 billion in 2022 [1]. Therefore, the applications of WSN network are increasing day by day in a considerable way. WSNs are used in different applications [2] like Environmental monitoring, Vehicle tracking, Health care monitoring, Smart building, Security and surveillance, Animal tracking, Precision agriculture, etc. WSNs are classified into five groups [3], depending on the deployment environment of sensor nodes: Terrestrial, Underground, Multimedia, Underwater, and Mobile. WSNs [4] include sensor nodes and base station (BS). The sensor nodes sense different parameters like humidity, temperature, voltage, light, pressure, soil makeup, etc. and send sensory observations to the BS using wireless channel. Sensor nodes are resource constrained with less processing capabilities, memory, battery, short communication range and bandwidth. Sensor nodes are deployed remote, hostile and unattended locations. Security for WSN is important because of resource constrained nodes, wireless channel used for communication and hostile deployment of nodes.

Security of WSN is provided in two levels [5]. Cryptographic techniques and firewalls are used to provide the protection from outside attackers of network in the first level. IDS is used to provide the protection from internal attackers in the second level. IDS is used to do intrusion detection only and not for prevention. Intrusion is an unauthorized access of the information, alter the information, drop some of the packets and forward to next nodes in the network. Intrusion detection is a mechanism for detecting intrusion activities in the network and raise alarm when intrusion is detected. The IDS is performed in four different techniques: Signature based IDS, Anomaly based IDS, Specification based IDS and Hybrid based IDS. Signature based IDS is used to detect the known attacks by identifying rules for attacks. Anomaly based IDS is used to identify the unknown attacks by using statistical, data mining, machine learning and artificial intelligence techniques. Specification based IDS detect the both known and unknown attacks by generating the rules manually. Hybrid based IDS is combinations of any two among the following techniques: signature based, anomaly based and specification based. All these IDS techniques are discussed in detail in the next section.

The WSNs are exposed to various kinds of attacks because of several constraints related to limited processing capabilities, finite battery power, limited storage space, narrow wireless bandwidth, short communication range and random deployment of sensor nodes. In WSN, adversary can easily compromises the sensor nodes and introduce attacks in WSN. The attacker can introduce attacks into the network at different layers of network. The detail information about the attacks at different layers is discussed in the next section. To defend against the attacks WSN requires IDS. The IDS proposed for the WSN must consider the issues related to constrained processing capabilities, limited energy availability and narrow bandwidth.

Many researchers conducted their work on IDS for WSN. Their work varies based on topology of the WSN and based on defense approach [6]. Majorly there are two different topologies used for WSN: Flat based and Cluster based. Physical structure of WSN network is also discussed in the next section. In IDS, defending against attack can be performed in two different ways: Centralized approach and Distributed approach. In centralized approach, intrusion detection is performed in BS. In Centralized approach, only single node is used to detect the attack. So there is a possibility to increase false positives. In distributed approach, detection of attacks is performed at multiple levels of the network: sensor node, cluster head (CH) and BS. In the first level, sensor node detects attacks and sends the attack information to the CH. The CH performs defense mechanism to identify the malicious sensor node and forward that information to the BS. The BS performs defense mechanism to identify malicious traffic from CH. Distributed approach has more communication overhead. In wireless network, more energy is consumed for communication and not for processing. So the distributed IDS approach consumes more energy for communication of IDS information from sensor to CH and CH to BS.

A detailed review on IDS for WSN is presented in this paper over the last decade as significant changes are observed during this period. Many survey papers are published on IDS in WSN [3, 5, 8, 44]. Hence, this survey paper differs from earlier efforts in the following ways:

- Abduvaliyev *et al*. [3] presented different attacks in WSN and also presents IDS mechanism for WSN, but it does not present the performance metrics required for IDS in WSN. Our survey presents performance metrics for IDS in WSN.
- Alrajeh *et al*. [5], Butun *et al*. [8] and Ghosal *et al*. [44] concentrate only on IDS approaches in WSN but not discuss about the attacks which are occur in WSN. Our paper presents taxonomy of security attacks in WSN.

The formation of this paper is represented as follows: Section II presents the architecture of WSN, section III presents the taxonomy of attacks in WSN, section IV elaborates the IDS mechanisms used to detect the attacks in WSN, section V contains information about performance metrics for measuring efficiency of IDS algorithms, section VI concentrates on the open research issues of IDS in WSN and conclusions of the survey is presented in section VII.

2. Architecture of WSN

WSNs are classified based on features deployed in sensor nodes. Some sensor networks contain uniformity in deployed sensors while others contain distinctions in the nodes based on the architecture. Common topologies of WSN [6] are flat based topology and cluster based topology.

2.1 Flat-based topology

In flat based topology [7], all the Sensor nodes perform same operation i.e. sense the event, process the sensed information, and transmit the information through multi-hop routing technique to the BS as represented in Figure 1. Protocols for flat based topology use flooding technique to maintain good quality route from source to the BS. For flat based topology, some routing protocols are defined, viz., Rumor-Routing, Sensor Protocols for Information via Negotiation (SPIN), Directed-Diffusion, etc. Intrusion detection can be performed at sensor nodes or may be in the BS in flat based topology.

2.2 Cluster based topology

Cluster based topology [7] contains three different elements: sensor node, CH and BS. Sensor nodes in the network form into groups and each group has one CH that can elect by the sensor nodes in the group based on energy available. Sensor nodes sense the environment, process that information and transfer to the CH. CH aggregate the all information which is from sensor nodes and sends to BS as represented in Figure 2. Based on cluster based topology, some routing protocols were defined: Low-energy adaptive clustering hierarchy (LEACH), Base station Controlled Dynamic Clustering Protocol (BCDCP), etc. In this topology intrusion detection is performed at sensor node or CH or BS or distributed manner.

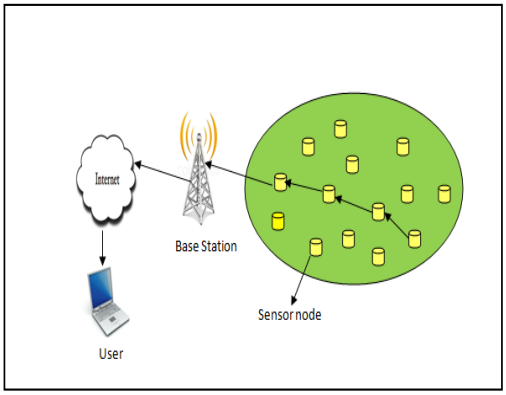

Figure 1. Flat based WSN

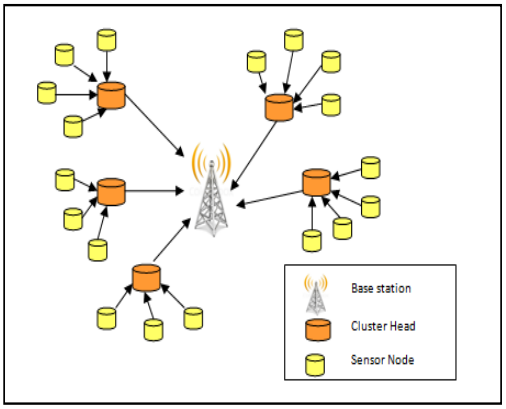

Figure 2. Cluster based WSN

3. Taxonomy of Attacks in WSN

Conventional security methods used for wired networks are computationally intensive and hence cannot directly implement for WSNs due to the resource constraint environment of WSNs. Security for information in WSN is provided by using Confidentiality, Integrity and Availability (CIA) [6]. Confidentiality provides the security from unauthorized access of information using cryptographic algorithms. Integrity protects against unauthorized modification and falsification of information using cyclic codes and Message Authentication Codes (MAC). Availability provides the information to right user at right time. It is difficult to provide availability of information and resources in resource constraint WSNs. Because of resource constrained environment of WSN, adversary can easily compromise with the node in the WSNs and perform different attacks to resource exhaustion at node.

Security attacks against WSNs are classified majorly into two types [8]: Passive attacks and Active attacks. In passive attack, adversary observes the communication link to access the data. Examples for passive attacks are: node tampering, traffic analysis and eavesdropping. In active attack, attacker observes communication link and modifies the data packet or drop the packets in middle of the communication. Active attacks are more dangerous compare to passive attacks. Active attacks were lunched at different layers of WSN. Taxonomy of attacks on layers of WSN is shown in Figure 9.

3.1 Physical Layer

In WSNs, "the physical layer performs different functions, such as generates carrier frequency, signal detection, modulation and data encryption to carry the information through wireless channel" [9]. Because of a wireless channel, the sensor node broadcast its information. Sensor node services are disturbed by jam or intercept the radio signals. WSN networks are deployed on to remote, hostile and unattended locations. So, there may be a chance of physical access of sensor nodes to access confidential information. The two main attacks of physical layer are jamming attack and node tampering attack.

3.1.1 Jamming attack

"Jamming Attack is caused by interfering the radio frequency of attacker nodes with the other nodes" [10]. The main objective of the jamming attack is to avert legitimate nodes from communication with little power. Jamming attacks utilize the shared nature of wireless channel to interrupt communication by decreasing the Signal to Noise Ratio (SNR). Santoro *et al*. [11] considered two types of jamming attacks: physical jamming and virtual jamming. Physical jamming was created using radio signal and virtual jamming was created by using request to send (RTS) and clear to send (CTS) signal.

Osanaiye *et al*. [12] proposed a hieratical approach for detecting jamming attacks with different forms. Jamming detector algorithm was installed on to the CH to identify compromised nodes in the cluster and also in the BS to detect the compromised CHs using packet interval time metric feature to identify unexpected modification in packet sequence using Exponential Weighted Moving Averages (EWMA). Del-Valle-Soto *et al*. [13] proposed two mechanisms for detecting reactive jamming attacks: connected mechanism and extended mechanism. In the connected approach, information of the performance metrics was collected directly from connected sensor nodes. The extended approach requires collector node which identifies performance parameters of all the sensor nodes in the WSN and perform compression on performance parameter of all the nodes in network. Sasikala *et al*. [14] proposed a method for identifying jamming attack using Artificial Bee Colony (ABC) by considering energy, packet loss, distance and packet delivery ratio.

3.1.2 Node tampering attack

In tampering attack, adversary may modify legitimate node to change the node as compromise node. Adversary can access the sensitive information such as security keys or data from the sensor node. Periyanayagi *et al*. [15] proposed a model for detecting tampering and cheating attack using swarm based trust node for tampering and cheating attack (SWTN-TC). Swarm Intelligence was used to select the Trust Node (TN) to detect tampered and cheating nodes. Each Session was classified as fair or cheating by TN by processing the session receipt using Cryptographic Puzzle Hiding Scheme (CPHS).

3.2 Link Layer

The link layer of WSN is performs framing, error control, data frame detection and medium access [4]. Attacks at link layer are collisions, Denial of Sleep, resource exhaustion and unfairness in allocation of channel [9].

3.2.1 Collision attack

A collision attack occurs while two nodes convey their information simultaneously with same frequency at same time. When packet collision occurs, it performs retransmission of collide packets [9]. An adversary intentionally perform the collision for the specific packets such as control packets results the costly exponential back-off. An adversary performs the collision by violating communication protocol rules and continuously transmits message.

3.2.2 Denial of Sleep attack

The Denial of Sleep attack is the link layer attack. It prevents the node from sleep mode. The sensor nodes consume more energy for transmitting and receiving the information to or from sensor node. Medium access control (MAC) protocols of WSN conserves energy of node using sleep mode. The adversary continuously transmits the control messages to the legitimate node to reduce the sleep time. Hence, more energy is consumed at nodes. Naik *et al*. [16] proposed defending mechanism to identify Denial of Sleep attack in WSNs. The author used zero knowledge protocol (ZKP) for checking the legitimacy of the sensor nodes which sensor node sends the sleep synchronization messages. Bhattasali *et al*. [17] proposed hierarchal model for detecting insomnia of sensor nodes and reduce power utilization and increase the life time of network.

3.2.3 Exhaustion Attack

Adversary performs recurring collisions and several retransmissions until node die. A Compromised node continuously requests or broadcast over the channel to drain the resources of the node [18].

3.2.4 Unfairness Attack

Unfairness is a fragile form of Denial of Service (DoS) attack [9]. This attack introduces the unnecessary delay in using MAC protocols to degrade performance of WSN.

3.3 Network Layer

Network layer of WSN performs routing the information from source sensor node to destination sensor node through intermediate sensor nodes (routers) [4]. Routing protocols selects the optimal path to transmit the packets. Adversary manipulates the routing protocols to introduce the network layer attacks with non-optimal path to reduce life time of a network. Network layer attacks are blackhole attack, misdirection attack, selective forwarding attack, wormhole attack, sinkhole attack and sybil attack [19].

3.3.1 Black hole attack

In black hole attack, attacker node publishes itself has a shortest path from source node to the destination node. Hence, source node uses path through the attacker node to send information to the destination node. The attacker node drops the all received packets in the network without forwarding to the destination

node. The IDS for detecting black hole attack in WSN was proposed in [26], [32], [33], [38], [39].

3.3.2 Misdirection attack

Misdirection attack is one of the DoS attacks. In misdirection attack, the attacker changes the path of the received packets to a node other than the destination node [20]. Forwarding traffic to the specific direction causes the resource exhaustion of sensor nodes throughout the path. Ahmad *et al*. [38] proposed improved K-means algorithm to identify misdirection attacks in WSNs.

3.3.3 Selective Forwarding attack

Selective forwarding attack is also known as grayhole attack. Selective forwarding attack is variation of a black hole attack. In block hole attack, attacker node announce itself has shortest path to the destination through the that node and drops all the packets which packets passes through that node. But in selective forwarding, compromised sensor node drops packets selectively. Most of the researchers detect the selective forwarding attack by making the assumption as malicious node drops packets which are coming from specific sender/destination or drops the packets based protocol used (drops all UDP packets or drops all TCP protocol) [21]. Detection of selective forwarding attack in WSN was proposed in [26], [32], [33], [62], [63].

3.3.4 Wormhole attack

In wormhole attack, attacker compromises the two sensor nodes in the different areas of WSN. Attacker creates the high bandwidth channel between two compromised nodes to access the packets from source sensor node [22].

3.3.5 Sybil attack

Sybil attack is also called impersonation attack. In sybil attack, adversary compromise the node in the network and compromised node masquerades as multiple nodes with false identities [22]. Wang *et al*. [49] and Le *et al*. [54] considered the Sybil attack for performing IDS in WSN.

3.3.6 Sinkhole attack

In sinkhole attack, an adversary compromises the nodes near to sink node or comprises the sink node to attract whole traffic in the WSN [22]. Detecting sinkhole attack in WSN was considered in [36], [46], [58].

3.4 Transport layer

Transport layer provides the logical connection among the applications running on two different sensor nodes. Transport layer protocols vulnerable to different attack: TCP SYN flooding attack and Desynchronization attack [6].

3.4.1 TCP SYN Flooding Attack

The TCP SYN flooding attack is a type of DoS attack. Transmission control protocol (TCP) is a transport layer protocol. TCP establishes the communication between two nodes by using 3-way handshake. The three messages (SYN, SYN-ACK, ACK) exchanged between the sensor nodes during the handshake to identify whether nodes ready for communication and exchange messages using sequence numbers. To introduce SYN attack, malicious node sends more number of SYN packets. After receiving SYN packets, the victim node sent the SYN+ACK packet and wait for ACK packet as response. Hence causes half-open connections at victim node. Victim node communicates with other nodes when TCP half open connection was timeout [23].

3.4.2 Session hijacking

Session hijacking is also Impersonation attack. In this attack, attacker impersonates the IP address of victim sensor node, identifies the sequence number of packet expected by the receiver sensor node and introduces DOS attack [23].

3.4.3 Desynchronization attack

Desynchronization is a DoS attack. Attacker introduces desynchronization attack to disturb communication between two end points and the attacker continuously modifies messages at both the sides of sensor nodes [6].

3.5 Application layer

The application layer protocols like HTTP, TELNET, SMTP and FTP transmit the user information. The attacker is very attractive with the application layer information because it directly contains user information. Application layer attacks consume more bandwidth and also consume sensor node energy. Application layer attacks in WSN are DoS and Deluge attacks [23].

3.5.1 DoS attack

In DoS attack of application layer, an attacker contradicts the services of the legitimate node by sending more number of empty messages to receiver sensor node to consume bandwidth and energy of sensor nodes [23].

3.5.2 Deluge attack

Deluge attacks also called reprogramming attack. Adversary installs malicious program (viruses, spywares, Trojan Horses and worms) on sensor node application or in operating systems. The malicious programs on the sensor node extend themselves through the network to slow down the network or to damage the network [23].

4. IDS in WSN

Intrusion detection techniques are classified based on functionality of the detection algorithms. Intrusion detection in WSN performed in four different ways [6] namely: signature based, anomaly based, specification based and hybrid based. All these techniques used to classify legitimate and attack traffic. Classification of IDS for WSN is shown in Figure 3.

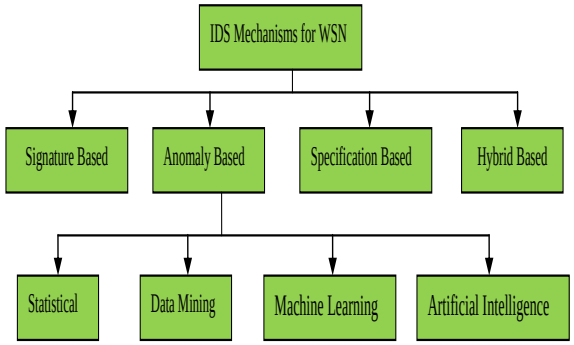

Figure 3. Classification of IDS techniques for WSN

4.1 Signature based detection

Signature based IDS are also known as misuse based or rule based IDS approach. Signature based IDS detects only known attacks. Nannan et al. [24] proposed rule based IDS for WSNs to generate class association rules using Genetic Network Programming (GNP). To differentiate with one rule to another rule authors uses the jaccard distance. Cho et al. [25] proposed partially distributed IDS for WSNs to detect DoS attacks. Author's uses the bloom filters (BF) to reduce the energy consumption for storing attack signature.

Hidoussi *et al*. [26] proposed misuse based IDS for WSNs for detecting selective forwarding attacks and black hole attacks. In this IDS, attack signatures are stored in the BS to reduce the energy consumption at sensor nodes. Berjab *et al*. [28] proposed distributed approach for performing intrusion detection and failure handling using fuzzy logic in Event Condition Action (ECA) for cluster based WSN. Author develops the rules by identifying the correlation on the multivariate attribute (MVA) and spatiotemporal attributes (STA). IDS was distributed to sensor nodes, cluster aggregator and CH. Authors used temporal similarity at sensor level, spatial similarity at cluster aggregator level, STA and MVA correlations used at CH level to detect the intrusions. Table.1 represents the information about Signature based IDS.

Signature based IDS increases the false alarm because it detects only known attacks but it can't detect the unknown attacks and it requires the memory to store the attack pattern. In WSN, sensor nodes have limited storage capacity, so it doesn't have that much memory to store the attack pattern. Signature based IDS were not suitable for WSN [29] because of limited storage capacity for storing attack signature in sensor nodes.

4.2 Anomaly based detection

Anomaly based IDS detect unknown attacks without knowing prior knowledge about the attack and also detect the known attacks. Anomaly based detection-based techniques are classified into four different categories based their functionalities [30]: Statistical based, Data mining based, Machine Learning based and Artificial Intelligence based. Anomaly based IDS were performed in two phases: training phase and testing phase. In the training phase, normal traffic and attack traffic given as input to the IDS model to learn about the normal traffic and attack traffic to classify normal traffic and attack traffic. In testing phases, test for the new traffic is normal or attacked.

4.2.1 Statistical based

In Statistical anomaly-based IDS, stochastic behavior of normal traffic was profiled by monitoring the network traffic periodically [31]. Anomaly score was calculated to detect the attack in the new traffic, compare anomaly score with the threshold value and generates the alarm when anomaly score is greater the certain threshold. Attack detection using statistical based anomaly detection performed using statistical measure (mean, standard deviation, variance), statistical models (logistic regression, auto regression) and statistical inference test (chi-square test, T-test) are used to determine whether the traffic is legitimate or not.

Ioannou *et al*. [32][33] proposed a model for IDS for resource constrained WSN using Binary Logistic Regression (BLR) to detect selective forwarding attack and blackhole attack. In these papers, authors creates different network scenarios using cooja network simulator by changing sink node position and gathers network traffic for normal case and attack case. Detection module was developed using BLR and deployed on to every sensor node to predict new traffic is a normal or attacked.

Osanaiye *et al*. [12] proposed a statistical approach to identify the jamming attacks in WSN. In this paper authors use the Exponentially Weighted Moving Averages (EWMA) to identify jamming attacks with received packet arrival feature from sensor node.

Han *et al*. [34] used two methods to detect malicious attacks in WSNs in energy efficient way: Game theory and Auto Regressive model. Game Theory model contains two players: attacker and defender. Attacker attacks the network and defender defends the network from malicious attacks. To perform defense to the attack in energy efficient way authors uses auto regression to detect when the attack may occur and what is the next attack node. To perform optimal defense strategy authors uses the Nash equilibrium solution.

J. W. Ho *et al.* [35] implemented a distributed model to discover the mobile node with malicious attacks in static WSN using Sequential Probability Ratio Test (SPRT). The basic idea of this model is to apply sequential hypothesis testing to realize the sensor nodes that are quiet for remarkably many time periods and block those sensor nodes from communication because of the static nodes are always with the neighbors and communicate with them.

Shafiei *et al.* [36] proposed two ways to detect and mitigation of sinkhole attack in WSNs. First way is to detect the attack region using centralized geo-sampling approach and next is for detecting sinkhole attack through distributed monitoring by investigating every neighbour node in WSN. Ballarini *et al.* [37] uses a Generalized Stochastic Petri Nets (GSPN) to identify deployment position of cnodes which are used only for detecting DoS attack in the cluster and notifies to the CH. Table 2 represents information about statistical based IDS.

Statistical based anomaly detection has advantage to provide accurate notification of malicious activities. It also has limitations: attacker can easily train statistical model to allow abnormal activities as normal, difficult to find out threshold and difficult to consider a greater number of features.

4.2.2 Data Mining based

Signature based IDS performance was dependent on the rules identified by the security experts. The process of Identification of rules was difficult, expensive and slow because of huge amount of network traffic. To avoid the limitations in specification-based IDS, Data mining techniques are used for IDS in WSNs. Data mining includes different approaches such as clustering, classification, association, sequence analysis and forecasting. All these approaches are used for IDS in WSN.

Ahmad *et al.* [38] proposed an improved K-means clustering for detecting blackhole and misdirection attacks in WSNs. The normal traffic and attack traffic was simulated using network

simulator 2 (NS2). Blackhole attack was detected by using sent traffic of a sensor node. The sent traffic of sensor node is the zero then that node is identified as blackhole node. Misdirection attack was detected by using delay of the received packet. If received packet delay is greater than threshold then misdirection attack was identified.

Kaur *et al*. [39] proposed IDS model for identifying blackhole attacks within WSNs using K-means and J48 decision tree. Initially, NS2 simulator was used to gather network traffic under normal and attack situation. Then altered K-means clustering was used to divide the network traffic into normal and attack. Result of K-means may even have false negatives. Therefore, J48 classification was applied to get more accuracy with classification of normal and attack traffic.

Coppolino *et al*. [40] proposed a distributed model for identification of sinkhole and sleep deprivation attacks in WSN. In this model, local detection module was installed in every node in WSN to perform preliminary IDS and central agent was deployed on BS to access results of locally performed intrusion detection activities and coordinated to LA.

Almomani *et al*. [41] used a eight different data Mining models (Naive Bayes, Decision Trees, Random Forests (RF), Support Vector Machine (SVM), J48, Artificial Neural Networks (ANN), K-Nearest Neighbor (KNN) and Bayesian Networks) are developed to detect DoS attacks (Blackhole, flodding, grayhole, scheduling). Data mining techniques applied on WSN-DS [42] after reducing the number of features. Finally authors observed high accuracy with Random Forest for detecting blackhole and grayhole, Naive bayes for detecting flooding attack and scheduling attack.

Li *et al*. [43] uses K-Nearest Neighbor (KNN) classification algorithm was used to detect the flooding attack in WSNs. In this paper Intrusion detection was performed with five different modules: wireless network interface module, data storage module, analysis and judgment module, and intrusion response module. Table 3 represents information about Data mining based IDS.

Data mining techniques overcome the limitations of non data mining techniques by using huge dataset for detecting the intrusions in WSNs. Data mining algorithms for IDS are less efficient when the data set contains missing data or bad data values.

4.2.3 Machine Learning based

Machine learning algorithms are used for IDS in WSNs. "Machine learning based anomaly IDS generate an explicit or implicit model of the analyzed patterns that are updated periodically for improving the system performance based on previous results" [44].

Xie *et al*. [45] proposed an online model to detect random faults and cyberattacks using hypergrid KNN algorithm. This model reduces the computational and communicational complexity by reformulating anomaly from detection region of hypersphere to detection region of hypercube. Garofalo *et al*. [46] developed a distributed model to detect sinkhole attacks in WSNs using Decision tree. Author's uses network simulator 3 (NS3) to generate normal traffic and attack traffic. In this, IDS is composed with local agents and central agents. Local agent deployed on to every sensor node in the WSNs and use threshold values to detect the intrusions in local sensor and sends the information to the BS. The BS contains central agent module to categorize traffic as normal or attacked.

Ma *et al*. [47] used NSL-KDD dataset for performing intrusion detection by using spectral clustering (SC) and deep neural network (DNN). SC was used to group the data instances into different clusters. Each cluster uses one DNN to perform classification of normal and attack traffic and finally aggregate the outputs of all DNNs.

Shamshirband *et al.* [48] proposed a distributed model to perform intrusion detection in WSN using game theory and fuzzy Q-learning approach. Game theory approach was used to detect and defense intrusions at sink node and BS to detect immediate attack and fuzzy Q-learning approach was used to adjust the game theory parameters to detect the future attacks.

Almomani *et al.* [42] generate the new IDS dataset (WSN-DS) for WSN using NS2 network simulator with five different cases: normal, blackhole attack, flooding attack, scheduling attack and grayhole attack. Authors used ANN to detect attacks in the WSN-DS. Wang *et al.* [49] proposed a model to detect the localization attacks in WSN. Author's uses stacked de-noising auto encoder to detect attacks which occurred at localization application. In this paper, authors simulated the WSN but doesn't specifies which network simulator was used. Qu *et al*. [50] proposed a model for detecting blackhole and flooding attacks using fuzzy C-Means (FCM), one class SVM and sliding window. Authors used EXata simulator to simulate WSN. In this paper, authors first performed normalization on test data using Z-score normalization, then FCM is used to identify the noise data, one class SVM was used to identify attack traffic which was similar to the normal traffic and finally applies the sliding window procedure on output of the one class SVM to identify whether the data is attacked or not.

Otoum *et al*. [51] proposed an IDS model for cluster based WSN. In this model intrusion detection was performed in CH by using two sub systems: RF, enhanced density based spectral clustering of applications with noise (E-DBSCAN). RF used to detect the known attacks and E-DBSCAN used for detecting unknown attacks.

Otoum *et al*. [52] conducts comparison on machine leaning based IDS and deep learning based IDS for WSN. Authors identified that, deep leaning based IDS gives high accuracy compare to the machine learning based IDS but deep learning based IDS takes more time to detect the attacks compare to the Machine learning based IDS.

Most of the researchers make use of KDD dataset to test IDS model in the offline for WSN. But KDD dataset is class imbalanced dataset. Because of imbalanced dataset doesn't give the accurate results. Tan *et al*. [53] used SMOTE algorithm to perform class imbalance and then uses Random forest algorithm to perform intrusion detection on KDDCup'99 dataset.

Le *et al*. [54] proposed a model for detecting blackhole, flooding, scheduling and grayhole using RF algorithm. Author's uses WSN-DS [42] dataset was used to train RF based machine learning model. Table 4 represents information about Machine Learning based IDS. "Machine learning methods require high

computing resources during the training and testing phases of anomaly detection, which is detrimental to the function of the resource constrained sensor nodes" [6]. But machine learning algorithms give high accuracy in detecting the intrusions.

4.2.4. Artificial Intelligence based

Artificial intelligence (AI) techniques are used for performing Intrusion detection in WSNs to perform automatic detection of attacks with reduced human intervention. Intrusion detection based on AI includes different techniques [55]: Genetic Algorithm (GA), artificial immune, ANN, and Swarm Intelligent.

Mansouri *et al*. [56] proposed a centralized approach to detect command injection attack, response attack, DoS attack and reconnaissance attack using ANN. Authors uses Evolutionary System (ES) and Gray Wolf Optimization (GWO) to get optimal weights of ANN. Gas pipeline and water pipeline dataset was used to perform training to the ANN**.**

Bitam *et al*. [57] proposed a distributed approach for detecting cyber attacks in WSN using AI with swarm intelligence. Authors show that AI with swam intelligence gives high accuracy and low false alarm with theoretical study.

Nithiyanandam *et al*. [58] simulate the WSN using NS2 network simulator and gather network traffic under normal scenario and attack scenario. Author proposed a model using ant colony optimization (ACO) and particle swarm optimization (PSO) to detect the sinkhole attack with high accuracy.

Sun *et al*. [59] proposed distributed IDS for WSN using adaboost, Artificial-fish-swarm-algorithm (AFS) and cultural algorithm (CA). An adaboost with hierarchal structures used in sensor nodes, CHs and sink nodes to perform anomaly detection. CA and AFS with back propagation is applies to perform miss-use detection at BS. Author uses NSL-KDD dataset to train the model.

Singh *et al*. [60] proposed energy efficient IDS for clustered WSNs by using GA. IDS were performed into four modules: data collection, intrusion information, intrusion detection and alert. The data collection module, sensor node traffic was monitored by its CH. The intrusion information module collects the intrusion data for justification. The intrusion detection module identifies the intrusions activity of the node based on threshold. The alert module informs about intrusion to the member sensors. A genetic algorithm was used to select agent nodes by using mutation parameter to spin the node energies. Table 5 represents information about AI based IDS. Intrusion detection using AI techniques gives high accuracy in WSN, but not easily scalable and can agonize from the concern of overfitting at the time of training.

4.3 Specification based detection

Specification based IDS [8] combines the benefits of each rule based and anomaly based detection techniques. In Specification based IDS, intrusion rules were developed manually to detect the known attacks. Specification based IDS also detect the unknown attacks based on the deviation from normal profile. Because of manual representation of rules specification based IDS gives low false positives but takes more time to develop the rules.

Farooqi *et al*. [61] proposed specification based IDS framework for flat WSNs. This framework operates in two modes: offline detection and online prevention. Offline detection used for detecting compromised nodes during the next epoch time. Online prevention provides protection to legitimate nodes from abnormal nodes. Specification based IDS gives the efficient result but this frame work requires more time to generate the rules manually.

4.4 Hybrid Approach

Hybrid based intrusion detection in WSN performing by combining signature based, anomaly based or specification based intrusion detection techniques to increase accuracy, detection rate and reduce false alarm rate. Sedjelmaci *et al*. [62] proposed a hybrid approach by using anomaly based approach and specification based approach to detect network layer attacks (hello flood, selective forwarding, blackhole and wormhole). Authors uses TOSSIM network simulator to simulate the WSN under normal and attack scenarios. Yan *et al*. [7] proposed hybrid IDS by combing anomaly based back propagation network (BPN) and misuse based intrusion detection techniques. Author's used KDDCup'99 dataset to apply anomaly and misuse detection techniques.

Alaparthy *et al*. [27] proposed distributed and light weight approach for detecting energy depletion attack by using signature based and anomaly based detection. Authors perform anomaly detection based on artificial immune system which is inspired from white blood cells in human body. Subba *et al*. [63] proposed hybrid approach for detecting intrusions in multiple layers of network. Specification based intrusion detection used by IDS agent to detect the intrusions sensor node level. Anomaly detection based on neural network module installed in the CH to classify the normal IDS agent and anomalous IDS agent. Hybrid intrusion detection approach uses the benefit of signature based, anomaly based and specification based approach. Hybrid intrusion detection approach increases accuracy but also increases complexity [6]. Table.6 represents information about Machine Learning based IDS.

Some of researchers perform intrusion detection by calculating trust value of the node. Ramesh Rao *et al*. [65] proposed Node Activities Learning (NAL) to track the runtime activities of the node to calculate trust value of node and predict the probability of the node offensiveness to protect the WSN from attacker.

The study of intrusion detection techniques in WSN reveals that majority of researchers apply the machine learning algorithms to perform intrusion detection in WSNs that are represented in Figure 4. But machine leaning algorithms takes more time to perform training and testing and also requires more memory to deploy the machine learning model [6]. From the study, it is identified that, intrusion detection can be performed in centralized approach or distributed approach. The centralized approaches take more burden at a detection node and also take more time to identify the intrusion. In Distributed approach, detection module is deployed on to the different levels (sensor node, CH, BS) of the WSN. Hence, it consumes more energy to

exchange the messages between different levels of nodes. Most of the Researchers use distributed approach to detect the intrusions is represented in Figure 5.

Some of researchers used the network intrusion detection dataset to check the accuracy of their own algorithm. Most of the researchers used KDDCup'99 dataset. But KDDCup'99 data set is developed for intrusion wired networks not for wireless networks. So KDDCup'99 is not suitable for WSNs. At present no suitable intrusion detection dataset for WSN. Some researchers create their own dataset by using network simulators and perform intrusion detection using simulated dataset. Most of researchers uses NS2 network simulator to simulate WSN under normal and attack scenario.

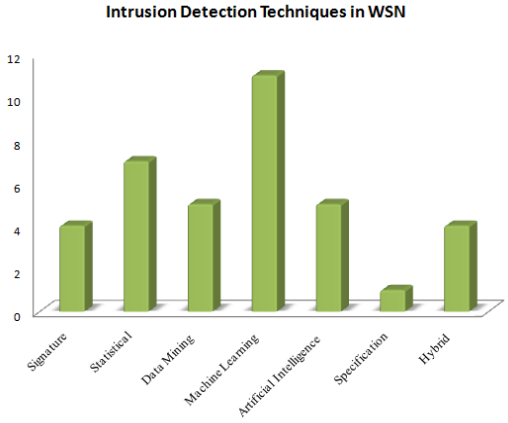

Figure 4. Intrusion detection techniques in WSN

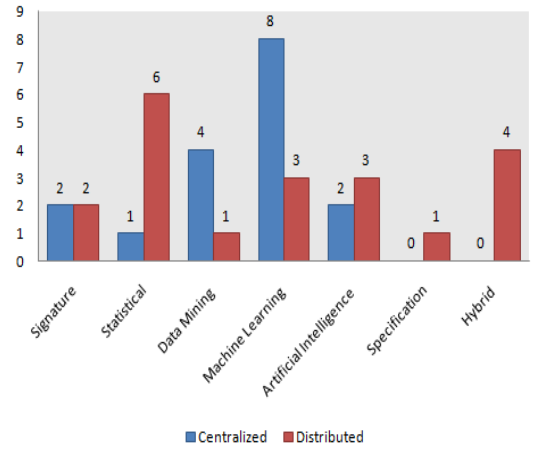

Figure 5. Intrusion detection approach in WSN

5. Performance Metrics for IDS in WSN

Performance of intrusion detection algorithm can be analyzed by using following measures: Confusion matrix, Receiver operating curves and Precision-Recall curve.

5.1 Confusion matrix

Intrusion detection application in WSN comes under the binary classification problem. The result of binary classification of IDS in WSN can be represented using 2×2 confusion matrix i.e. shown in Figure 6. An abnormal flow is treated as Positive and normal flow is treated as negative. Confusion matrix contains four sections: True Positives (TP) represents the amount of actually abnormal flows predicted correctly as Abnormal flows. TN represents the amount of actually normal flows predicted correctly as normal flows. False Positives (FP) represents the number of actually normal flows incorrectly classified as abnormal flows. False Negatives (FN) represents the number of actually abnormal flows incorrectly classified as normal flows. Effectiveness of intrusion detection algorithm was measured using following metrics: detection accuracy, True Positive Rate (TPR), False Positive Rate (FPR), True Negative Rate (TNR), False Negative Rate (FNR), F1 score and geometric mean index.

		Detected Flows: Abnormal	Detected Flows: Normal
Actual Flows	Abnormal	TP	FN
	Normal	FP	TN

Figure 6. Confusion matrix for binary classification

5.1.1 *Detection Accuracy*

Detection accuracy (DA) represents the percentage of instances correctly classified. Accuracy of intrusion detection algorithm was calculated using Equation (1)

$$DA = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \quad (1)$$

5.1.2 *TPR*

TPR also called sensitivity, recall and detection rate. TPR represents the percentage of actually abnormal flows identified correctly. Equation (2) represents the formula for calculating TPR.

$$TPR = \frac{TP}{TP + FN} \quad (2)$$

5.1.3 *TNR*

TNR also called as specificity and selectivity. TNR represents the percentage of actual normal cases identified correctly i.e. represented in Equation (3).

$$TNR = \frac{TN}{TN + FP} \quad (3)$$

5.1.4 *FPR*

FPR represents the probability of false alarm. FPR represent the percentage of actual abnormal flows predicted as normal flows. Equation (4) represents the formula for calculating FPR.

$$FPR = \frac{FP}{FP + TN} \quad (4)$$

5.1.5 *FNR*

FNR represents the percentage of normal flows predicted as abnormal flows. Equation (5) represents the formula for calculating FNR.

$$FNR = \frac{FN}{FN + TP} \quad (5)$$

5.1.6 Precision

It also called as positive predictive value. It is represents the ratio between TP and sum of the positive predictions. Equation (6) represents the formula for calculating TPR.

$$Precision = \frac{TP}{TP + FP} \quad (6)$$

5.1.7 F1 score

F1 Score is the harmonic mean of Precision and Recall i.e. represented in Equation (7). Compare to the accuracy, f1 score is the best metric to check effectiveness of intrusion detection algorithm when IDS model uses unbalanced input dataset.

$$f1\ score = \frac{2 * Precision * Recall}{Precision + Recall} \quad (7)$$

5.1.8 Geometric mean

Intrusion detection algorithms can be evaluated using geometric mean of precision and recall i.e. represented in Equation (8). Geometric mean reaches to high when both precision and recall are high.

$$Geometric\ mean = \sqrt{Recall * precision} \quad (8)$$

Geometric mean of TPR and TNR also considered as intrusion detection metric for unbalanced datasets. This metric introduced as Geometric Mean Accuracy Index (GMAI) in [64] i.e. represented in Equation (9).

$$GMAI = \sqrt{TPR * TNR} \quad (9)$$

Any intrusion detection algorithm must yield high Accuracy, TPR, TNR, f1 score, geometric mean and low false alarm rate and FNR.

5.2 Receiver Operating Curves (ROC)

ROC is a graph which represents the trade-off between TPR and FPR. The Area under ROC curve shows the detection accuracy of the model. More area under the ROC curve of any intrusion detection means that algorithm gives good results. In this graph X-axis represents FPR and Y-axis represents TPR. The ROC curve of the Intrusion Detection model can't below the 45^0 line which represents the minimum prediction line. Figure 7 is an example of ROC. In Figure 7, the model which represents the blue line gives high-quality results because of area under this curve is greater than the red line.

5.3. Precision-Recall Curve (PR curve)

PR curve is a graph which represents the trade–off between precision (Y-axis) and recall (X-axis) for different thresholds. The IDS algorithm which gives more area under the PR curve that algorithm gives good results. A PR curve is the best measure to investigate performance of an intrusion detection algorithm when IDS model uses unbalanced dataset. A simple PR curve is shown in Figure 8. From the Figure 8 it is identified that Algorithm 2 gives the best results compared to the Algorithm 1.

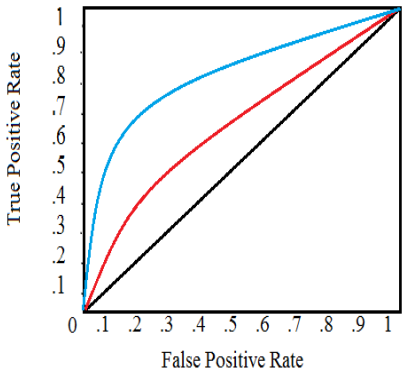

Figure 7. Simple ROC curve

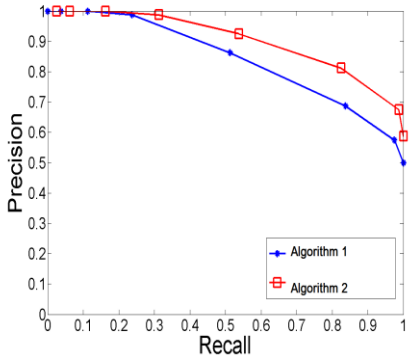

Figure 8. Simple PR curve

6. Future Directions for IDS in WSNs

For performing proper training and assessment about attacks, model requires benchmark dataset for WSN. From the literature it is understood that, there is no benchmark dataset specifically for WSN. So, there is a requirement to develop labeled dataset for WSN to perform training and assessment about the attacks.

Most of the researchers used machine learning algorithms to perform intrusion detection in WSN. A machine learning algorithm need more time to perform training and testing and also requires more memory space to deploy machine learning model in sensor nodes. So, there is a scope to develop compact machine learning model for performing intrusion detection in WSN to decrease memory space to deploy a model.

The maximum number of existing techniques concentrates only on specific type of attack focused about specific layer of the WSN, without concentrating on other layer attacks. So, it is essential to develop cross-layer IDS that can detect the different attacks which may occur in different layers of WSN.

7. Conclusion

In this paper, the architecture of WSNs, viz., flat based WSN and cluster based WSN is presented. The study indicates that the Cluster based WSN reduces the energy consumption on sensor node because most of the computations are performed in CH

which has high processing, memory and battery. We also discussed about the attack based on the layered structure of WSN. IDS for WSN was performed on four different techniques viz., Signature based, anomaly based, Specification based and hybrid mechanism. We discussed all these mechanisms and also briefed research papers which use these techniques. Performance of intrusion detection algorithm is measured using detection accuracy, TPR, false alarm rate and f1 score. Performance metrics for Intrusion Detection System in WSN are also presented in this paper. Finally the future directions for IDS in WSN are briefly presented.

References

[1] P. Rawat, K. Singh, H. Chaouchi, and J. Bonnin, "Wireless Sensor Networks: A Survey on Recent Developments and Potential Synergies," J. Supercomput., Vol. 66, No. 1, pp. 1–48, Oct. 2013.

[2] J. Yick, B. Mukherjee, D. Ghosal, "Wireless Sensor Network Survey," Computer Networks, Vol. 52, No. 12, pp. 2292-2330, 2008.

[3] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong,''On theVital Areas of Intrusion Detection Systems in Wireless Sensor Networks,'' IEEE Commun. Surveys Tuts., Vol. 15,No. 3, pp. 1223–1237, 3rd Quart., 2013.

[4] I.F. Akyildiz et al., "Wireless Sensor Networks: A Survey," Computer Networks, Elsevier Science, Vol. 38, No. 4, pp. 393-422, 2002.

[5] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review," Int. J. Distrib. Sensor Netw., Vol. 9, No. 5, Jan. 2013.

[6] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of Service Defence for Resource Availability in Wireless Sensor Networks," IEEE Access, Vol. 6, pp. 6975–7004, 2018.

[7] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network," 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, pp. 114-118, 2010.

[8] I. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Commun. Surveys Tuts., Vol. 16, No. 1, pp. 266–282, 2014.

[9] J. Sen, "A survey on wireless sensor network security," Int. J. of Commun. Netw. and Information Security, Vol. 1, pp. 55–78, 2009.

[10] S. Shanthi and E. G. Rajan, "Comprehensive Analysis of Security Attacks and Intrusion Detection System in Wireless Sensor Networks," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, pp. 426-431, 2016.

[11] D. Santoro, G. Escudero-Andreu, K.G. Kyriakopoulos, F.J. Aparicio-Navarro, D.J. Parish and M. Vadursi, "A Hybrid Intrusion Detection System for Virtual Jamming Attacks on Wireless Networks," Measurement, Vol.109, pp.79-87, 2017.

[12] O. Osanaiye, A.S. Alfa and G.P. Hancke,"A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks," Sensors, Vol. 18, No. 6, p. 1691, 2018.

[13] C. Del-Valle-Soto, L. J. Valdivia and J. C. Rosas-Caro, "Novel Detection Methods for Securing Wireless Sensor Network Performance under Intrusion Jamming,"2019 International Conference on Electronics, Communications and Computers (CONIELECOMP), Cholula, Mexico, pp. 1-8, 2019.

[14] E. Sasikala and N. Rengarajan," An Intelligent Technique to Detect Jamming Attack in Wireless Sensor Networks (WSNs)," International Journal of Fuzzy Systems, Vol. 17, No. 1, pp. 76–83, 2015.

[15] S. Periyanayagi and V. Sumathy, "Swarm-Based Defense Technique for Tampering and Cheating Attack in WSN using CPHS," Personal and Ubiquitous Computing, Vol. 22, No. 5-6, pp. 1165-1179, 2018.

[16] S. Naik and N. Shekokar, "Conservation of Energy in Wireless Sensor Network by Preventing Denial of Sleep Attack," Procedia Computer Science, 45, 370–379, 2015.

[17] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network," Int. J. Comput. Appl., Vol. 40, No. 15, pp. 19–25, 2012.

[18] A. Diaz and P. Sanchez, "Simulation of Attacks for Security in Wireless Sensor Network," Sensors, Vol. 16, No. 11, p. 1932, 2016.

[19] I. Tomic and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," IEEE Internet of Things Journal, Vol. 4, No. 6, pp. 1910-1923, Dec. 2017.

[20] R. S. Sachan, M. Wazid, D. P. Singh, A. Katal and R. H. Goudar, "Misdirection attack in WSN: Topological Analysis and An Algorithm for Delay and Throughput Prediction," 2013 7th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, pp. 427-432, 2013.

[21] W. Wang, S. Zhang, G. Duan, and H. Song, ''Security in Wireless Sensor Networks,''in Wireless Network Security. Berlin, Germany: Springer, pp. 129–177, 2013.

[22] H. K. Patil and T. M. Chen, "Wireless Sensor Network Security," Computer and Information Security Handbook, 317–33, 2017.

[23] T.G. Lupu, I. Rudas and N. Mastorakis, "Main Types of Attacks in Wireless Sensor Networks," WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering, no. 9, 2009.

[24] Nannan Lu, Yanjing Sun, Hui Liu, and Song Li, "Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks," Journal of Sensors, vol. 2018, Article ID 5948146, 8 pages, 2018.

[25] E. J. Cho, C. S. Hong, S. Lee, and S. Jeon, "A Partially Distributed Intrusion Detection System for Wireless Sensor Networks," Sensors, vol. 13, no. 12, pp. 15863-15879, 2013.

[26] F. Hidoussi, H. Toral-Cruz, D. Boubiche, K. Lakhtaria, A. Mihovska, and M. Voznak, "Centralized IDS Based on Misuse Detection for Cluster-Based Wireless Sensors Networks," Wireless Personal Communications, Vol. 85, No. 1, pp. 207-224, 2015.

[27] V. T. Alaparthy and S. D. Morgera, "A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory," IEEE Access, Vol. 6, pp. 47364-47373, 2018.

[28] N. Berjab, H. H. Le, C. Yu, S. Kuo and H. Yokota, "Hierarchical Abnormal-Node Detection Using Fuzzy Logic for ECA Rule-Based Wireless Sensor Networks," 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan 2018, pp. 289-298.

[29] R. Mitchell and I. R. Chen, "A Survey of Intrusion Detection in Wireless Network Applications," Computer Communications, Vol. 42, pp. 1–23, 2014.

[30] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly Detection in Wireless Sensor Networks: A Survey," J. Netw. Comput. Appl., Vol. 34, No. 4, pp. 1302–1325, 2011.

[31] H.-J. Liao, C.H. Richard Lin, Y.C. Lin, and K.Y. Tung, "Intrusion Detection System: A comprehensive review," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013.

[32] C. Ioannou, V. Vassiliou and C. Sergiou, "An Intrusion Detection System for Wireless Sensor Networks," 2017 24th International Conference on Telecommunications (ICT), Limassol, pp. 1-5, 2017

[33] C. Ioannou and V. Vassiliou, "An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression," In Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM '18). ACM, New York, NY, USA, pp. 259-263, 2018.

[34] L. Han, M. Zhou, W. Jia, Z. Dalil, and X. Xu, "Intrusion Detection Model of Wireless Sensor Networks based on Game Theory and an Autoregressive Model," Inf. Sci., Vol. 476, pp. 491–504, 2018.

[35] J. W. Ho, M. Wright, and S. K. Das, "Distributed Detection of Mobile Malicious Node Attacks in Wireless Sensor Networks," Ad Hoc Networks, Vol. 10, No. 3, pp. 512–523, 2012.

[36] H. Shafiei, A. Khonsari, H. Derakhshi, "Detection and Mitigation of Sinkhole attacks in Wireless Sensor Networks", Journal of Computer and System Sciences, Vol. 80, No. 3, pp. 644-653, 2014.

[37] P. Ballarini, L. Mokdad, and Q. Monnet, "Modeling Tools for Detecting DoS Attacks in WSNs," Security and Communication Networks, Vol. 6, No. 4, pp. 420–436, Apr. 2013.

[38] B. Ahmad, W. Jian, Z. Anwar Ali, S. Tanvir, M. Sadiq Ali Khan, "Hybrid Anomaly Detection by Using Clustering for Wireless Sensor Network," Wireless Personal Communications, Vol. 106, No. 4, pp. 1841–1853, 2018.

[39] G. Kaur and M. Singh, "Detection of Blackhole in Wireless Sensor Network based on Data Mining,"2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), Noida, pp. 457-461, 2014.

[40] L. Coppolino, S. DAntonio, A. Garofalo and L. Romano, "Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks," 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Compiegne, pp. 247-254, 2013.

[41] I. Almomani and M. Alenezi, "Efficient Denial of Service Attacks Detection in Wireless Sensor Networks," Journal of Information Science and Engineering, Vol. 34, No. 4, pp. 977–1000, 2018.

[42] I. Almomani, Bassam Al-Kasasbeh and Mousa AL-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," Journal of Sensors, Vol. 2016, 16 pages, 2016.

[43] Wenchao Li, Ping Yi, Yue Wu, Li Pan, and Jianhua Li, "A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network," Journal of Electrical and Computer Engineering, Vol. 2014, 8 pages, 2014.

[44] A. Ghosal and S. Halder, "A Survey on Energy Efficient Intrusion Detection in Wireless Sensor Networks," Journal of Ambient Intelligence and Smart Environments, Vol. 9, no. 2, pp. 239–261, 2017.

[45] M. Xie, J. Hu, S. Han and H. Chen, "Scalable Hypergrid k-NN-Based Online Anomaly Detection in Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 8, pp. 1661-1670, 2013.

[46] A. Garofalo, C. Di Sarno , V. Formicola, "Enhancing Intrusion Detection in Wireless Sensor Networks through Decision Trees," In: Vieira M., Cunha J.C. (eds) Dependable Computing. Lecture Notes in Computer Science, Vol 7869. Springer, Berlin, Heidelberg, EWDC 2013.

[47] T. Ma, F. Wang, J. Cheng, Y. Yu, and X. Chen, "A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks," Sensors, Vol. 16, No. 10, p. 1701, 2016.

[48] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah and A. Abraham, "Cooperative Game Theoretic Approach using Fuzzy Q-learning for Detecting and Preventing Intrusions in Wireless Sensor Networks," Eng. Appl. Artif. Intell., Vol. 32, pp. 228–241, 2014.

[49] H. Wang, Y. Wen and D. Zhao, "Identifying Localization Attacks in Wireless Sensor Networks Using Deep Learning," Journal of Intelligent & Fuzzy Systems, Vol. 35, No. 2, pp. 1339–1351, 2018.

[50] H. Qu, L. Lei, X.Tang, and P. Wang, "A Lightweight Intrusion Detection Method Based on Fuzzy Clustering Algorithm for Wireless Sensor Networks," Advances in Fuzzy Systems, Vol. 2018, 12 pages, 2018.

[51] S. Otoum, B. Kantarci and H. T. Mouftah, "Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications," IEEE Sensors Letters, Vol. 1, No. 5, pp. 1-4, Oct. 2017

[52] S. Otoum, B. Kantarci and H. T. Mouftah, "On the Feasibility of Deep Learning in Sensor Network Intrusion Detection," IEEE Networking Letters, 2019.

[53] X. Tan, S. Su, Z. Huang, X. Guo, Z. Zuo, X. Sun and L. Li, "Wireless Sensor Networks Intrusion Detection Based on SMOTE and the Random Forest Algorithm," Sensors, Vol. 19, No. 203, p. 203, 2019.

[54] T. Le, T. Park, D. Cho and H. Kim, "An Effective Classification for DoS Attacks in Wireless Sensor Networks," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, pp. 689-692, 2018.

[55] N. A. Alrajeh and J. Lloret, "Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, Vol. 9, No. 10, 6 pages, 2013.

[56] A. Mansouri, B. Majidi and A. Shamisa, "Metaheuristic Neural Networks for Anomaly Recognition in Industrial Sensor Networks with Packet Latency And Jitter for Smart Infrastructures," International Journal of Computers and Applications, 2018.

[57] S. Bitam, S. Zeadally and A. Mellouk, "Bio-Inspired Cybersecurity for Wireless Sensor Networks," IEEE Communications Magazine, Vol. 54, No. 6, pp. 68-74, 2016.

[58] N. Nithiyanandam, P. Latha Parthiban, B. Rajalingam, "Effectively Suppress the Attack of Sinkhole in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique," International Journal of Pure and Applied Mathematics, Vol. 118, No. 9, pp. 313-329, 2018.

[59] X. Sun, B. Yan, X. Zhang, and C. Rong, "An Integrated Intrusion Detection Model of Cluster-based Wireless Sensor Network," Plos One, Vol. 10, No. 10, 2015.

[60] S. Singh and R. S. Kushwah, "Energy Efficient Approach for Intrusion Detection System for WSN by Applying Optimal Clustering and Genetic Algorithm," In Proceedings of the Int. Conf. on advances in info. Commu. tech. & comput.—AICTC '16, pp. 1–6, New York, 2016.

[61] A. H. Farooqi, F. A. Khan, S. Lee, and J. Wang, "A Novel Intrusion Detection Framework for Wireless Sensor Networks," Personal and Ubiquitous Computing, vol. 17, No. 5, pp. 907–919, 2013.

[62] H. Sedjelmaci, S. M. Senouci and M. Feham, An Efficient Intrusion Detection Framework in Cluster-based Wireless Sensor Networks, Security and Communication Networks, vol. 6, no. 10, pp. 1211–1224, 2013.

[63] B. Subba, S. Biswas and S. Karmakar, ”A Game Theory Based Multi Layered Intrusion Detection Framework for Wireless Sensor Networks,” Intenational Journal of Wireless Information Networks, pp. 1-23, 2018.

[64] C. Madhusudhana Rao, M. M. Naidu, “A Model for Generating Synthetic Network Flows and Accuracy Index for Evaluation of Anomaly Network Intrusion Detection Systems,” Indian Journal of Science and Technology, vol. 10, no. 14, 2017.

[65] K. Ramesh Rao, S. N. Tirumala Rao, and P. Chenna Reddy, “Node Activities Learning (NAL)Approach to Build Secure and Privacy-Preserving Routing in Wireless Sensor Networks,” International Journal of Communication Networks and Information Security (IJCNIS), Vol. 10, No. 3, December 2018.

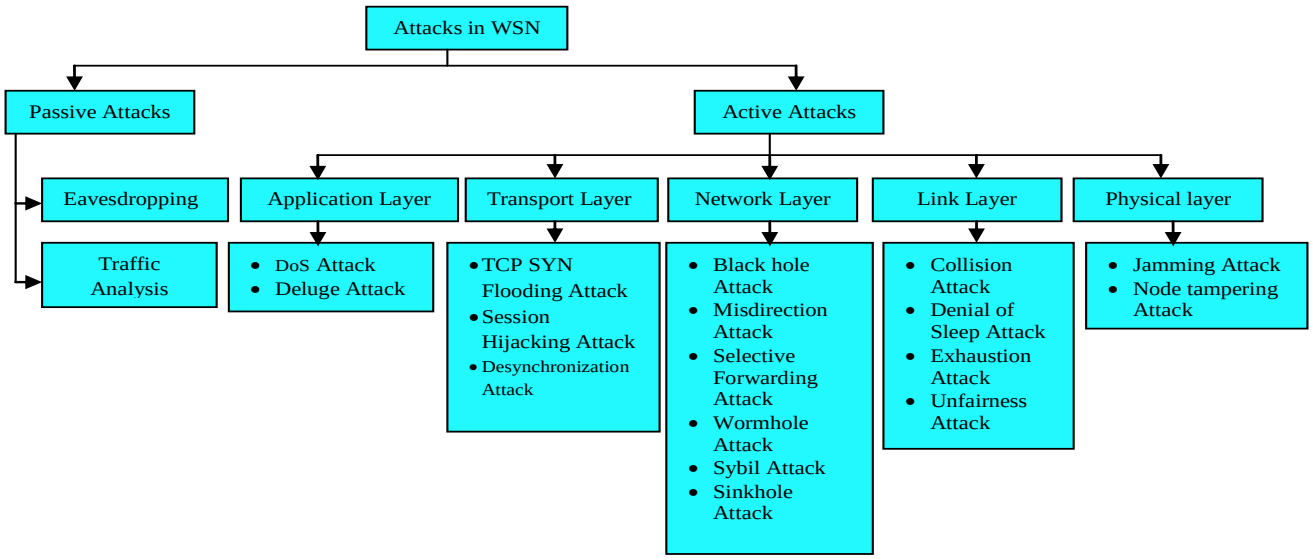

Figure 9. Taxonomy of attacks in WSN

Table 1. Signature based IDS in WSN

Authors	Defense Approach	Attacks Considered	Technique used	Dataset
Nannan et al. [24]	centralized	• DoS • User to Root • Remote to Local • Probe	• GNP	NSL-KDD
Hidoussi et al.[26]	Centralized	• Black hole • Selective forwarding	• Reception and delay rule • Sub-List of CH member's nodes rule • Information loss rule	Collected from NS2 network simulator
Cho et al. [25]	Distributed	• DoS	• BF	Collected from NS2 network simulator
Berjab et al. [28]	Distributed	• No specific attack defined	• STA correlation • MVA correlations	Real world dataset

Table 2. Statistical based IDS in WSN

Authors	Defense Approach	Attacks Considered	Technique used	Dataset
Han et al. [34]	Centralized	• Malicious	• Auto regressive • Game theory	MAT Lab
Ioannou et al. [32][33]	Distributed	• Selective forwarding • Blackhole	BLR	Collected from Cooja network simulator
Osanaiye et al. [12]	Distributed	• Jamming	• EWMA	CRAWDA
Shafiei et al. [36]	Distributed	• Sink hole	• Geo-statistical	Castalia simulator (OMNeT++)
J. W. Ho et al. [35]	Distributed	• DoS	• SPRT	
Ballarini et al. [37]	Distributed	• DoS	• GSPN	Collected from NS2 network simulator

Table 3. Data mining based IDS in WSN

Authors	Defense Approach	Attacks Considered	Technique used	Dataset
Ahmad et al. [38]	Centralized	• Blackhole • Missdirection	• Improved K-means	Collected from NS2 network simulator
Kaur et al. [39]	Centralized	• Blackhole	• K-means • J48	Collected from NS2 network simulator
Almomani et al. [41]	Centralized	• Flooding • Grayhole • Blackhole • Sceduling	• Naive Bayes • Decision Trees • RF • SVM • J48 • ANN • KNN • Bayesian Networks	WSN-DS
Li et al. [43]	Centralized	• Flooding	• KNN	Test bed
Coppolino et al. [40]	Distributed	• Sinkhole • Sleep deprivation	• Decision Tree	Collected from NS3network simulator

Table 4. Machine Learning based IDS in WSN

Authors	Defense Approach	Attacks Considered	Technique used	Dataset
Almomani et al. [42]	Centralized	• Flooding • Grayhole • Blackhole • Sceduling	ANN	Collected from NS2 network simulator (WSN-DS)
Ma et al. [47]	Centralized	• DoS • User to Root • Remote to Local • Probe attack	• SC • DNN	NSL-KDD
Wang et al. [49]	Centralized	• Sybil • Reply • Interference • Collision	• Stacked De-noising Auto Encoder	Network simulator used But not specifies simulator name
Qu et al. [50]	Centralized	• Blackhole • Flooding	• FCM • One class SVM • Sliding Window	EXata network simulator
Otoum et al. [51]	Centralized	• DoS • User to Root • Remote to Local • Probe	• RFt • E-DBSCAN	Collected from NS2 network simulator
Otoum et al. [52]	Centralized	• DoS • User to Root • Remote to Local • Probe	• RBM	Collected from NS2 network simulator
Tan et al. [53]	Centralized	• DoS • User to Root • Remote to Local • Probe	• SMOTE • Random Forest	KDD Cup'99
Le et al. [54]	Centralized	• Flooding • Grayhole • Blackhole • Sceduling	• RF	WSN-DS
Shamshirband et al. [48]	Distributed	• DoS	• Game Theory • Fuzzy Q-learning	Collected from NS2 network simulator (WSN-DS)
Xie et al. [45]	Distributed	• Cyber • Random Faults	KNN	Test bed
Garofalo et al. [46]	Distributed	• sinkhole	• Decision tree	Collected from NS3network simulator

Table 5. Artificial Intelligence based IDS in WSN

Authors	Defense Approach	Attacks Considered	Technique used	Dataset
Mansouri et al. [56]	Centralized	• Command injection • Response • DoS • Reconnaissance	GWO ANN	Gas pipeline
Nithiyanandam et al. [58]	Centralized	• Sinkhole	• ACO • PSO	Collected from NS2 network simulator
Bitam et al. [57]	Distributed	• Cyber	• Swarm Intelligence	Theoretical analysis
Sun et al. [59]	Distributed	• DoS • User to Root • Remote to Local • Probe	• Artificial-fish-swarm-algorithm • Cultural algorithm	NSL-KDD
Singh et al. [60]	Distributed	• Flooding	• GA	Collected from MAT LAB

Table 6. Hybrid based IDS in WSN

Authors	Defense Approach	Attacks Considered	Technique used	Dataset
Sedjelmaci et al. [62]	Distributed	• Selective forwarding • Hello flood • Blackhole • Wormhole	• Anomaly based (SVM) + Specification based	TOSSIM
Yan et al. [7]	Distributed	• DoS • User to Root • Remote to Local • Probe attack	• Anomaly based (BPN) + Signature based	KDDCup'99
Alaparthy et al. [27]	Distributed	• Energy depletion	• Anomaly based (Immune Theory) + Specification based	Collected from Cooja network simulator
Subba et al. [63]	Distributed	• Selective forwarding • Blackhole • Wormhole • DoS • Sybil	• Anomaly based (ANN) + Specification based	Collected from NS2 network simulator