Computer Systems Science & Engineering
DOI:10.32604/csse.2022.018518
Article

Tech Science Press

Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks

Vasaki Ponnusamy[1,*], Mamoona Humayun[2], N. Z. Jhanjhi[3], Aun Yichiet[1] and Maram Fahhad Almufareh[2]

[1]Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Kampar, Malaysia
[2]Department of Information Systems, College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia
[3]School of Computer Science and Engineering (SCE), Taylor's University, Selangor, Malaysia
[*]Corresponding Author: Vasaki Ponnusamy. Email: vasaki@utar.edu.my
Received: 11 March 2021; Accepted: 08 May 2021

Abstract: Internet of Things (IoT) devices work mainly in wireless mediums; requiring different Intrusion Detection System (IDS) kind of solutions to leverage 802.11 header information for intrusion detection. Wireless-specific traffic features with high information gain are primarily found in data link layers rather than application layers in wired networks. This survey investigates some of the complexities and challenges in deploying wireless IDS in terms of data collection methods, IDS techniques, IDS placement strategies, and traffic data analysis techniques. This paper's main finding highlights the lack of available network traces for training modern machine-learning models against IoT specific intrusions. Specifically, the Knowledge Discovery in Databases (KDD) Cup dataset is reviewed to highlight the design challenges of wireless intrusion detection based on current data attributes and proposed several guidelines to future-proof following traffic capture methods in the wireless network (WN). The paper starts with a review of various intrusion detection techniques, data collection methods and placement methods. The main goal of this paper is to study the design challenges of deploying intrusion detection system in a wireless environment. Intrusion detection system deployment in a wireless environment is not as straightforward as in the wired network environment due to the architectural complexities. So this paper reviews the traditional wired intrusion detection deployment methods and discusses how these techniques could be adopted into the wireless environment and also highlights the design challenges in the wireless environment. The main wireless environments to look into would be Wireless Sensor Networks (WSN), Mobile *Ad Hoc* Networks (MANET) and IoT as this are the future trends and a lot of attacks have been targeted into these networks. So it is very crucial to design an IDS specifically to target on the wireless networks.

Keywords: Internet of Things; MANET; intrusion detection systems; wireless networks

1 Introduction

Computer system must ensure Confidentiality and integrity against network security attacks. Jhanjhi et al. [1] describes that interconnectivity of huge number of devices and excessive usage of internet and data sharing increase the chances of security. Wanda et al. [2] refers to intrusions as an act of disrupting the network traffic by compromising the integrity and confidentiality of computer systems.

Tartakovsky et al. [3] describe Intrusion detection as the process of detecting and analyzing intrusions in a network by monitoring the traffic of a computer device or network for signs of intrusions that can be triggered by intruders, while IDs is defined as a system that is either represented in software or hardware to accommodate the process of detecting and analyzing intrusions in a network. Liao et al. [4] categorizes the various forms of IDs, such as host-based, network-based, wireless-based, network behavior analysis, and mixed IDs. According to Anthi et al. [5], a simple IDs consists of sensors, an analysis engine, and a reporting system to allow data collection, analysis, and detection of anomalies in the network, as well as generating a warning to report the detected intrusion in the system.

Since IDs consists of many components and features, a detailed analysis on these as a complete survey could contribute to the literature. This survey paper differs from others in the literature by providing a comparison between wired and WNs and providing the taxonomy of IDs in wired and WNs as shown in Fig. 1. This survey can benefit those embarking into IDs for WNs and mainly in IoT and any *ad hoc* networks. The paper is organized by providing a comparison between wired and wireless IDS in Section 2. Section 3 covers the IDS architectures that covers the data collection methods, detection techniques and deployment strategies. The wireless IDS design challenges and recommendations is discussed in Section 4. The paper in concluded in Section 5.

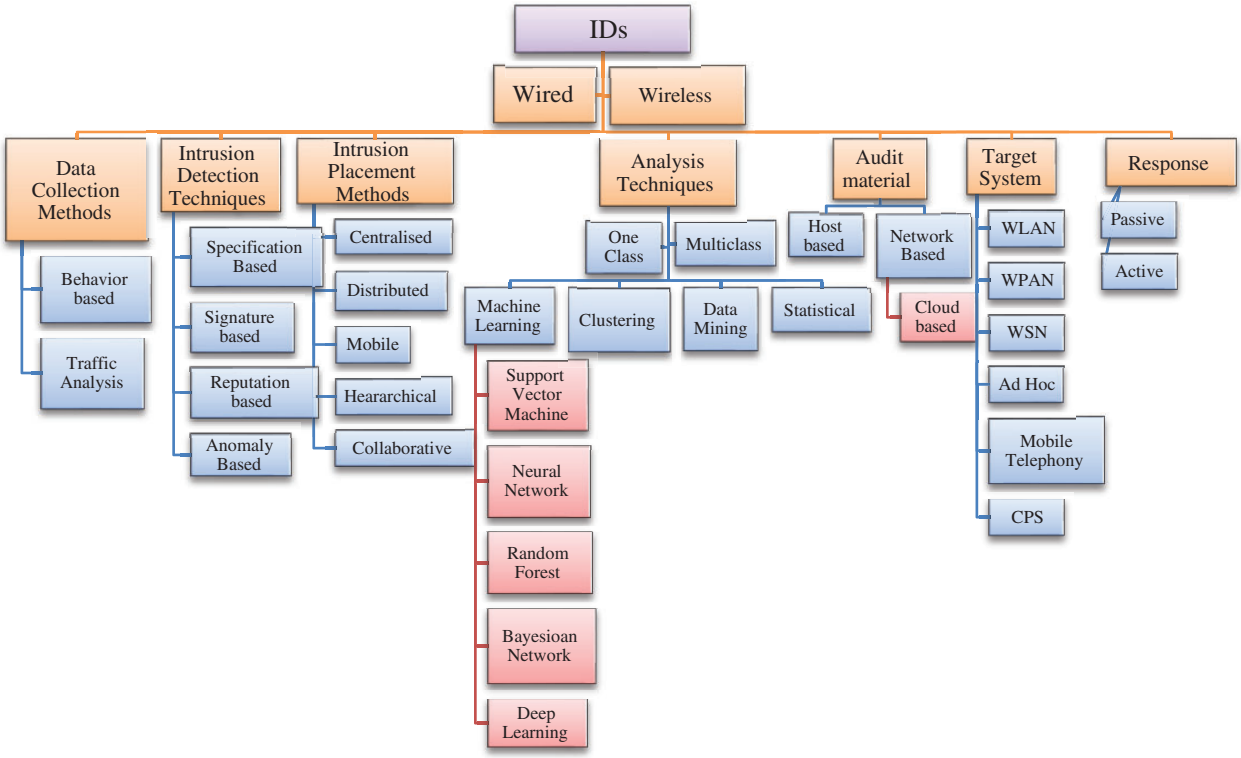

Figure 1: Taxonomy of IDs

2 Comparison between Wired and Wireless *Ad Hoc* IDSs

Ad hoc and IoT WNs consists of very power constrained devices that work on the wireless medium most of the time. Although IoT devices can communicate in peer to peer fashion like an ad-hoc network; most IoT devices talk to a centralized server (similar to Software Defined Network (SDN)) for device management and coordinations. To the best of our knowledge most of the research area in IDS focuses on traditional wired networks. Applying the wired network research of IDS at WNs may not be feasible due to the architectural differences of *ad hoc* networks. Traditional security countermeasures and privacy enforcement cannot be directly applied to *ad hoc* networks technologies due to the three fundamental aspects: (1) limited computing power of *ad hoc* network components, (2) the high number of interconnected devices and (3) sharing of data among users and objects [6]. Moreover, intrusion response to WNs depends on the type of intrusion, network protocols and applications in use and the confidence in the evidence, which is different from wired networks. The main challenge is the nature of WNs, unlike wired network, in WNs centralized access control is hard to be implemented due to the distributed nature of WNs. Wireless IDs will need to collect as much protocol data from the WNs as needed. Moreover, in WNs, there are specific vulnerabilities in physical and data link (Medium Access Control (MAC) vulnerability) layer which was not really attempted in designing wired IDS. Therefore, just deploying a wired IDS into wireless IDS would be just a false hope as it may not be able to detect some specific wireless attacks especially at data link layer. Moreover, deploying IDS in *ad hoc* networks is not as easy as it is anticipated and a detailed analysis of this challenges needs to be addressed before proposing a suitable IDS in wireless *ad hoc* networks [7]. Some of the challenges of IDS in *ad hoc* wireless are given below

- Frequent change of topology in *ad hoc* networks
- Open protocol which is vulnerable to many attacks—Since there is no fixed wired connection to the nodes in *ad hoc* networks, any adversary can join and leave the network anytime. It is hard to detect the attack nodes since the protocol is very open.
- Hard to detect by just looking at MAC address (wireless IDS survey)—Although there can be some mechanisms to detect the MAC address of the attack nodes, the node can easily change the MAC address since MAC address configuration in wireless just works by software configuration.
- Nodes are always mobile—It is very hard to deploy a centralized IDs since the nodes in *ad hoc* networks are keep moving and therefore a centralized IDS is not feasible.
- Resource Limitation of wireless nodes and wireless channels—Most of the times, nodes in *ad hoc* networks comprises of tiny devices with limited processing and storage capability which hinders the deployment of IDS in these resource constrained devices. Moreover *ad hoc* networks depend on wireless network such Wi-Fi, Bluetooth, ZgiBee or other mediums which has constraint in channel bandwidth allocation.
- Very high false positive and false negative—The dynamic organization of the network in *ad hoc* networks yields more false positive and false negative than wired networks

2.1 Wired and Wireless IDS Architecture

The wired or standard IDS architecture used to connect all the devices with a cable. The IDS console will play the role to monitor and analyze the network traffic. When traffic or packet is coming from the internet, the router will pass the data to the IDS server, the IDS server will do the traffic collection process and machine learning process. Basically, the IDS do not drop any packet since the job of IDS is to collect and analyze the data. The wired IDS required more component and device for the network setup, it mainly includes router, switch, IDS console, IDS server, and other end devices. Fig. 2a shows the wired IDs architecture

The wireless IDS architecture looks like a wired IDS architecture, but the difference is use of wireless access point for the network connectivity. The wireless IDS architecture is more convenient to the *ad hoc* network devices since most of the *ad hoc* network devices are using a wireless sensor to make the connection. Due to this, the communications between devices are exchanged in 802.11 packets that is very different from Ethernet frames (in terms of traffic headers and attributes). Furthermore, the typical components in a wireless IDS are the console, database server, and sensors. The network setup of wireless IDS might be easier since there are fewer cable will be installed. As a conclusion, the wireless IDS is more suitable for investigating the *ad hoc* network traffic and IDS architecture [8]. Fig. 2b shows the wireless IDS architecture.

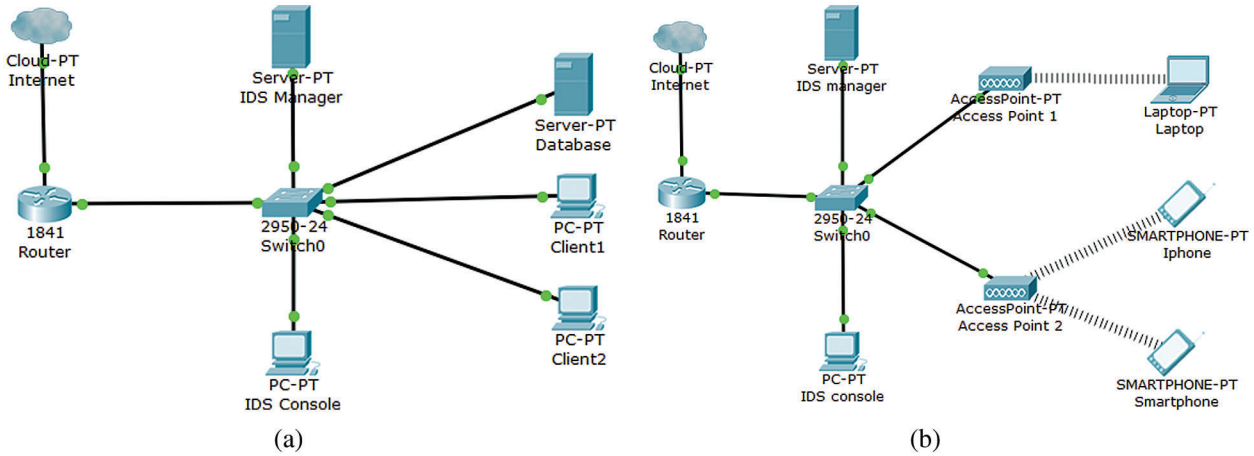

Figure 2: (a) Wired IDS architecture, (b) Wireless IDS architecture

3 IDs Architectures in Wireless *Ad Hoc* Networks

Although IDS is used to detect any intrusion, it has its own downside. The main issue with the IDS technologies is the accuracy of the detection. The accuracy of the IDS technologies can be measured by two parameters, false positive (FP) and false negative (FN). FP is generated when the system identified an intrusion, but it is actually not. For FN it is generated when the system does not detect any intrusion but in fact, intrusion happened. The other way to look at FN is that the system fails to detect the intrusion. To contemplate on the security of a system, a large number of security system administrator tend to choose to decrease FNs and increase FPs [9].

So, in order to propose and implement a suitable IDS in wireless *ad hoc*, a detailed analysis of IDS architecture is crucial. As shown in Fig. 1, this paper presents a survey of IDS in terms of data collection methods, detection techniques, IDS placement methods and analysis techniques. The literature presented is extracted from both traditional wired IDS as well as wireless IDS in place as most of these techniques does not differ much between wired and wireless. The uniqueness of this paper lies in the design challenges and recommendation for wireless IDS and the traffic analysis methods to study the feasibility of existing datasets available.

3.1 Intrusion Data Collection Methods

Data collection in wired and wireless network for the purpose of intrusion detection can be either collected from the behavior based or traffic analysis. Behavior based data collection is normally focusing much on the performance of the system such as Windows error reporting, web server performance, console log files [10], CPU usage, energy consumption and many other such similar data. This kind of

behavior data collection is very suitable when the area of analysis is not very much related to network data. For example, in order to perform malware detection at the operating system level, behavior analysis is the much-preferred solution. But behavior-based data collection will not be effective when detecting network related attacks as most of these attacks can only be shown at the respective network, transport, or data link layer. In this kind of situations, traffic analysis has greater advantage. Using traffic analysis, attack and non-attack data can be generated from the different Open System Interconnection (OSI) layers. Different layers would reflect different kinds of data. For example, at the network layer, source and destination IP address, time to live, packet length are some examples of relevant data to network attacks. Whereas at the transport layer; port no, sequence number and flags can uniquely represent the deviation from normal to abnormal data. So, this is the reason why for most of the network related attacks like Denial of Service (DOS), syn flooding, botnet and others, traffic data is more significant. In most of the wireless system more specifically in *ad hoc* and IoT, traffic based collection method is better than behavior based collection method [11].

There are a lot of traffic analysis related data already available which consists of attack and non-attack data. KDD cup is one such example which has about 22 different attacks related to network and transport layer which will be discussed in detail in Section 3.4. There are other related datasets available such as Predict 2014, Caida 2014, Kyoto Dataset 2014, ICS Attack Dataset 2014 and Adfa intrusion detection datasets 2014 [12].

3.2 Intrusion Detection Techniques

This section describes the commonly used intrusion detection techniques

3.2.1 Signature Based

Based on the survey, Liao et al. [4] describes IDS as an organized matching pattern that is used to detect the intrusion. There are several mechanisms used to detect in which they are differentiated by the representation and matching algorithms used. The approaches used are like pattern recognition, expert systems, state transition analysis and colored petri nets [13]. Signature based is one of the simplest and most effective method in detecting attacks but not well at detecting unknown attacks. And it also has a big challenge to keep the signatures up to date whilst a time-consuming approach [4]. But alternately signature based IDS produces less false positive signals as this system only responds to bad behavior nodes. The system must look for very specific signatures and the dictionary must provide signature and every specific attack vectors. This kind of IDS can work on univariate data like bytes transmitted, system history and also on multivariate data that has specific sequences [14]. One major challenge in this approach is to create a huge list of signatures to produce better prediction of attacks. But huge signature database requires longer processing and also incurs longer delay. So an optimal signature size and performance is essential in this kind of IDS [14]. Signature based intrusion detection (Fig. 3) works similar like antivirus in which it can detect all known signatures or attack patterns but becomes of no use when unknown attacks are present. SNORT is one good example of signature-based IDS in which the header information like source address, destination address and ports are used as signatures and the options field like payload is used to analyze the network traffic that corresponds to the signature. Kumar et al. [15,16] developed signature based IDS using virtual machine platforms to detect intrusions in the cloud.

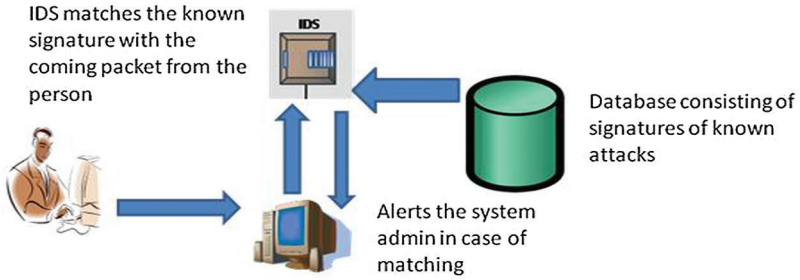

Figure 3: Signature-based detection IDS reacts to incoming attacks [17]

3.2.2 Anomaly Based

In Anomaly based intrusion as shown in Fig. 4, a normal profile of the network traffic is kept in the system. An intrusion is detected when the system detects an unusual traffic that deviates from the normal profile traffic. The common techniques used here are data mining, neural networks, and statistics. Training data that is created by supervised, semi-supervised and unsupervised is needed in order to create a normal profile data. Anomaly-based intrusion detection is further categorized into three specific domains: statistical-based, knowledge-based and machine learning-based [18,19] as shown in Fig. 5.

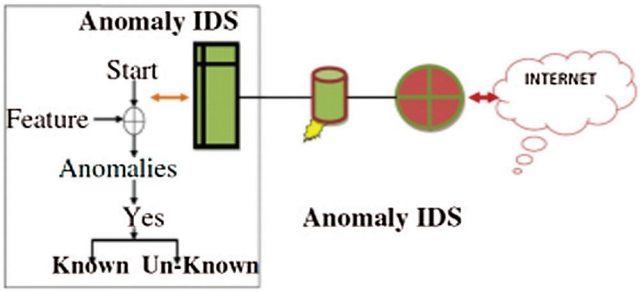

Figure 4: Anomaly based IDs [20]

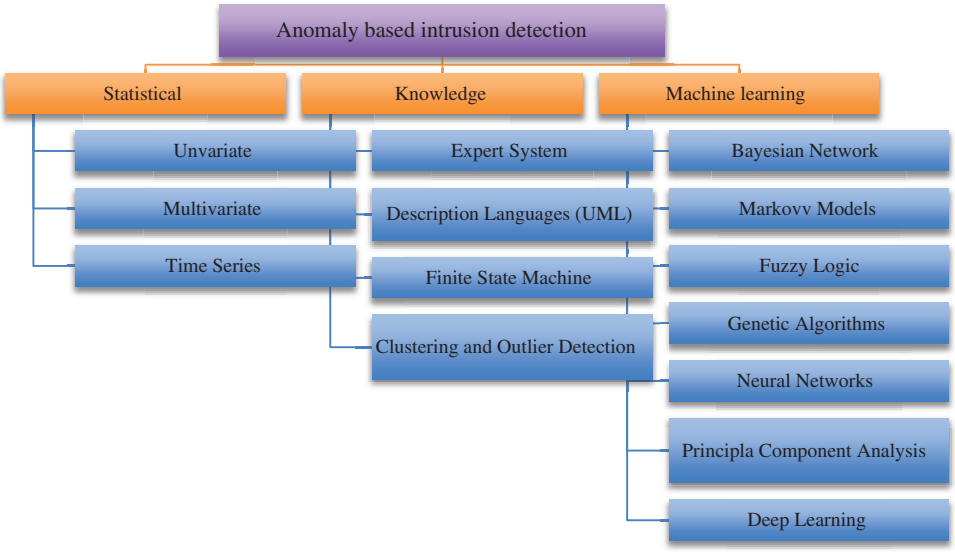

Figure 5: Classification of anomaly based IDs according to detection algorithms [21]

Based on statistical based anomaly IDS, the network traffic behavior profile is created. The profile is set as a reference when the network traffic is running in normal condition. The IDS will continue comparing the new profile data with the reference created earlier. When the profile shows a significant mismatch from the reference, then the traffic is flagged as abnormal. Whereas in knowledge-based anomaly IDS, the intrusion is detected by using the current network traffic or data whether being in the normal condition or in abnormal condition. Knowledge based intrusion can be performed by using expert system, description languages like Unified Modelling Language (UML), Finite State Machine (FSM) and clustering algorithms [22].

Machine learning based is more automatic in the sense that the system is able to learn the network profile and use it to detect any intrusive activities in the network. Machine learning based IDs is discussed in further detail in the following section due to its popularity. In 1959, Arthur Samuel defined Machine learning (ML) as "field of study that gives computers the ability to learn without being explicitly programmed". Basically, there are two things that the ML do that is classified and predict the data depends on the properties of the data that ML learns during the training phase. Also, ML requires an objective. The three main learning approaches in ML is unsupervised, semi-supervised, and supervised. Among the common method of these approaches is using support vector machine which is presented in Bhatti et al. [23].

Artificial neural network (ANN) is designed to work like the human brain. This has made the ANN to be much more capable than the usual machine learning models. A neural network consists of artificial neurons called units in each of the layers. The unit in a layer is connected to each of the unit in the next layer. An ANN has at least three layers, the input layer, hidden layers, and the output layer. The input layer serves as the way for the ANN to receive information and the output unit will respond accordingly after the information is being processed and learned. The hidden layers are located between the input layer and the output layer. There could have one or multiple hidden layers in ANN that structure most of the artificial brain. There is one more important feature in the ANN which is called a weight. Every connection in ANN has a weight and its value could be either positive or negative. The main objective of ANN is to learn and retrain the information in compliance with the input data and the output data [24]. ANN has been applied in some of the areas such as image processing and character recognition.

Some ANN based IDS have been done and a survey was carried to compare the different ANN models in Shah et al. [25]. One of the ANN model used is the Back Propagation Neural Network (BPNN). Many researchers prefer to use this model due to the advantages it provides. Shah et al. [25] has used this model because of the precise prediction and finer perseverance. The learning approach they used in BPNN is supervised learning. In their experiment, the authors find out that the time taken required for the model to train by using one hidden layer is shorter than using two layers. From the experiment, the authors also noticed that the model has problem of local minima and need more time to recover. The BPNN model showed good results in detecting known and unknown attacks but it also need great number of epoch and hence requires much time to train. It is also needed to define a state to end the training because too much training will worsen the performance of the model. Ullah et al. [26] uses Self-Taught Learning (STL) that consists of two stages which is unsupervised feature learning and the classification on labeled data using NSL-KDD dataset. On the other hand, Shone et al. [27] employed non-symmetric auto-encoder and random forests developing an unsupervised IDs that improved the detection rate while reducing the training time tremendously. The research was carried out using NSL-KDD dataset as well. Tang et al. [28] conducted deep learning intrusion detection using software defined network whereby the system was implemented in the SDN controller. This SDN controllers should be able to monitor the open-flow switches and collect their statistics as and when needed to increase the detection accuracy. Whereas, Yin et al. [29] employed recurrent neural network-based classification using NSL-KDD cup dataset separating the training and testing data that can effectively evaluate the intrusions in both binary and multiclass classification.

A lot of framework has been used for deep learning networks whereby [30] used H_2O framework for its application using Python and Scala. The implementation could cover wide range of interfaces, but only

limited number of models are supported and it is less flexible. Luckow et al. [31] used Tensorflow using Python for its application. The work could provide fast long short-term memory (LSTM) training and could support to visualize network but the training phase is slower compared to other Python based frameworks. Luckow et al. [31] also used Python based framework for IoT application whereby this work supports various models and fast LSTM training on GPU while Komar et al. [32] used Caffe framework

Anomaly based IDs is very good at detecting new and unanticipated vulnerabilities but are less dependent on operating system. But anomaly-based IDs can produce low detection accuracy due to constant change of activities and are normally not available when new profiles are being built. One key advantage of anomaly-based IDs is, it does not really look for any specific activities which means it does not need to fully specify all attack vectors and does not require the dictionary to be fully up to date. But this can also possibly cause more false positive signals. The system can also be vulnerable during the testing or profiling phase. In anomaly based detection, the normal behavior must be updated regularly since the network behavior changes frequently [33].

3.2.3 Specifications Based

Specification based intrusion detection focuses more on anomaly at the system level as compared to anomaly-based IDS that looks for anomaly at user profiles or data flows. But it works in the similar way whereby it defines the normal behaviors and detects anomaly when the system deviates from the normal behavior. This IDS produces lesser false positives than anomaly-based IDS since the system learns that only what legitimate behaviors defined by the expert is classified as normal and otherwise it is classified as abnormal. In another word, this system only works well only with the bad behaviors that disrupts the defined specifications in the system. The system is also effective in the sense that no training phase is required that makes it available immediately. The only disadvantage is that a lot of effort is required to define the formal specifications. This kind of IDS is effective in detecting insider attacks as it looks for abnormal behaviors in the system mainly on the system disruptions. On the other hand, it is not effective in detecting outsider attacks because it is mainly taking actions performed by insider and it is very much application centric. It is a kind of anomaly detection without having specific user, group or data profiles. The legitimate behaviors are defined by human and anything that deviates from this is specified as misbehaving nodes. This kind of IDS is suitable for nodes that is resource constraint whereby user, group or data profiles cannot be stored [14]. Sobh [34] points out that anomaly based intrusion detection looks for bad behavior effects whereas misuse detection looks for bad behaviors. In this case specification-based IDS combines both characteristics by manually specifying certain specifications that is constraint to detect legitimate system behavior.

3.2.4 Reputation Based

This kind of IDS is different from the earlier IDS discussed as this IDS normally looks for selfish nodes rather than looking for malicious nodes. But in the event that a misbehavior node is detected, the reputation manager has to look for ways to look into guarding the network in order to keep the reputation. One main challenge in this system is the distribution of the challenge score. Example of challenge scores are like packets sourced over packets destined, packets forwarded over packets sourced and many more. This kind of approach is suitable for large networks where *a priori* trust knowledge is not feasible. Reputation management is very suitable for *ad hoc* networks like Vehicular Area Network (VANET) and MANET [14].

3.3 IDs Architectures in Ad Hoc *Networks*

This section describes the architecture of IDs in *Ad hoc* networks

3.3.1 Audit Material

As we know, IDS can be deployed in every single node for monitoring node performances which is known as Host-based IDS (HIDS) (Fig. 6a) and can also be deployed in the entire network environment which is known as Network-based IDS (NIDS) (Fig. 6b). NIDS normally looks for intrusions like DOS attacks and port scans that attempt to disrupt network activities. A HIDS collects data from one host and

analyze it to detect intrusive event. This sort of IDS usually requires the host to install a small program to generate system logs or audit traits of operating system and analyzes the system behavior of nodes like looking at system files, network events, system calls, and modification on host kernels and also behavior of the program. When any deviation happens from the normal behavior, an intrusion is detected in this particular host. The chosen parameters will determine the effectiveness of the HIDS [35]. A summary of IDS architecture is shown in Fig. 7.

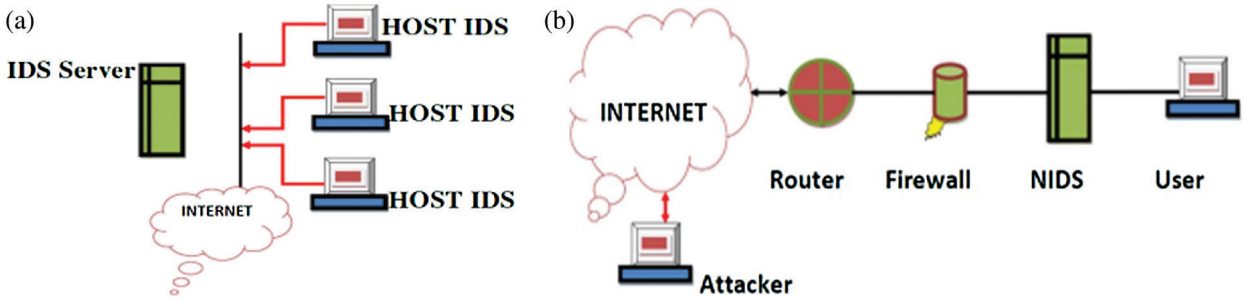

Figure 6: (a) Host based IDs [20], (b) Network IDs [20]

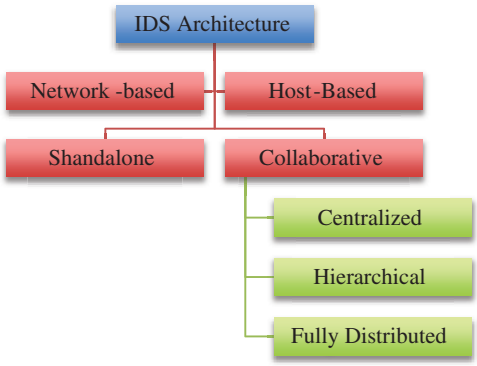

Figure 7: IDS placement architecture

A Distributed IDS (DIDS) is essentially an IDS which contains multiple IDS such as HIDS, NIDS, etc. It is most likely to be deployed in a large network which require different types of IDS to monitors the network traffics for intrusive events. DIDS uses detection components and correlation managers to connect and combine information gathered from those IDSs. DIDS is able to make use of both anomaly and signature-based intrusion detection, granting it the ability to detect both known and unknown attacks from the hackers [36]. NIDS normally inspects IP and transport layer headers employing either anomaly based or signature based IDs [37]. These HIDS and NIDS can be deployed using several different architectures.

3.3.2 Stand-alone IDs

Standalone architecture is very similar in concept as NIDS whereby IDs runs in every single node. The decision is made based on the information collected from the independent node. Node do not communicate or cooperate in order to make IDS decisions and therefore no information is exchanged between nodes. In this kind of IDS, nodes within the same network does not have any information on activities on other nodes as no alert information is shared among nodes. This approach may not be a very viable solution unless each node can run independently on its own without any limitations in terms of processing and storage capacity. Moreover, this approach is more suitable for flat architecture as compared to hierarchical architecture.

This IDS is not a suitable solution for MANET and IoT as information collected by each node is not sufficient to detect malicious events [38].

3.3.3 Collaborative IDs

A collaborative IDS is combination of several HIDS, and NIDS deployed over a large network that communicates with each other or to a centralized system for network monitoring purposes. In a collaborative IDS, the individual system can collect intrusion data, analyze and respond by itself or can be sent to a central system or even can be distributed to multiple systems amongst each other. Therefore, a collaborative IDS can be a centralized IDS, distributed IDS and can be a hierarchical IDS system too. This kind of collaborative IDS systems is useful since it can detect known and unknown attacks as it has both NIDS and HIDS as a whole [39].

3.3.4 Centralized IDs

In centralized IDS as shown in Fig. 8, one central node acts as the coordinating node whereby all other nodes act as detecting nodes which produces alerts locally. These alerts are then sent to the central server for analysis and decision making. DIDS [40] is one example of centralized IDS in which multiple IDS are put into one single system to detect intrusions in the entire network. Each local IDS would collect any abnormal activities within the individual system then converts it into a uniform format and forwards to the centralized agent for analysis. DShield is another example of centralized IDS which collects logs from firewall and IDS systems deployed globally. Any users of DShield can submit their logs to the DShield database which would be processed centrally by the DShield database. The analysis generated from the central database would report on attack events, vulnerable ports and any other vulnerabilities. NSTAT is another such example of distributed collection and centralized coordination of attacks. It works on client-server basis whereby the client is responsible for collecting and processing the audit trails and sending them to the central server. Whereas the server is responsible in integrating them and making analysis. Centralized IDS poses one major challenge as most of the analysis and decision is made on the central point of control. Any disruption of service on the single central node will hinder the performance of the entire system. Moreover, since data collection and alerts is performed at every single node, nodes must have sufficient capacity when huge volume of data enters [41].

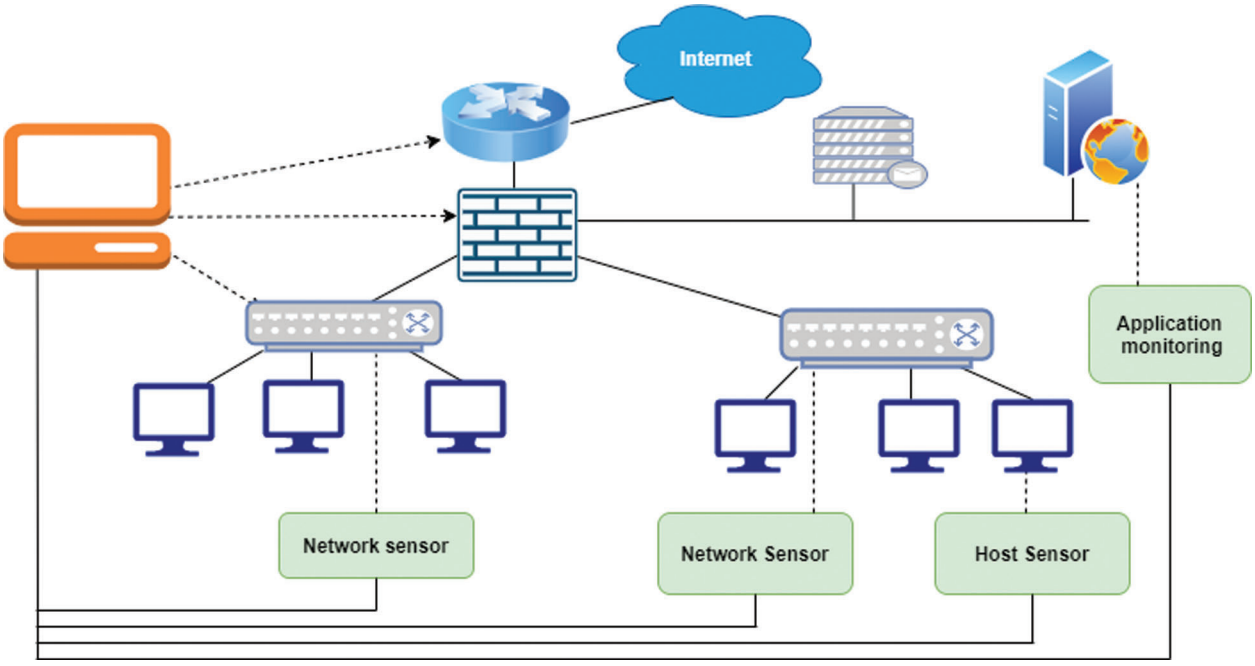

Figure 8: Centralized IDs [42]

3.3.5 Distributed IDs

Distributed IDS as presented in Fig. 9, is a much-preferred solution for IoT and MANET as the nature of them is distributed. In distributed IDS every node participant in response by having an agent running in each of them [43]. Agent plays important roles by collecting information from every node, detecting intrusion and finally making response decisions. But neighboring IDS agents can collectively make decisions when a conclusive decision cannot be made by one single agent. This is known as Cooperative Distributed IDS (CDIDS) [44]. Sanjay et al. [45] proposed a distributed IDS to detect DDoS attacks in cloud environment by deploying mutual agent-based approach. The cloud is divided into multiple regions and IDS agents in each region is responsible for notifying other regions if any intrusion is detected in its own region. Severity level is calculated in each region from the alerts received from other regions. New attacks detected based on the severity level is added to the rule-based system for collaborative use.

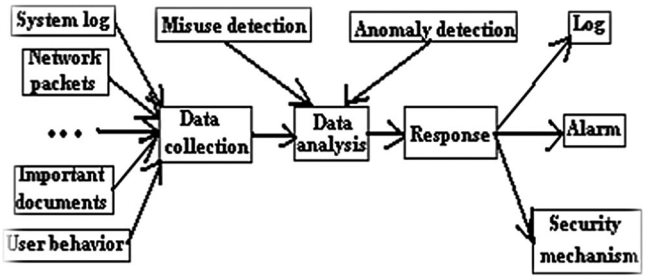

Figure 9: Distributed IDs [46]

3.3.6 Hierarchical IDs

Since centralized IDS is not scalable in nature, hierarchical architecture is proposed for that reason. In hierarchical architecture, nodes join into group of similar nature such as geography, administrative control, similarity in software platforms and types of intrusions. In hierarchical IDS, the entire system is classified into clusters by having one single node as cluster head in each cluster. All other nodes report to the cluster head in their respective cluster. Every single node is equipped with an IDS agent responsible for monitoring and deciding intrusions in its local node. A cluster head is also responsible for its local node as well as globally to collect intrusion data from its member nodes and deciding on the response event. In some cases, the analysis from the cluster head nodes will be further sent to the higher nodes for further processing [47].

3.3.7 Mobile agents for IDs

MANET also introduces mobile agents (MA) in its IDS deployment. Some nodes deployed as mobile agents to perform one specific task whereas all other nodes perform more functions. Due to its mobility nature, one or more mobile agents are distributed in each network. Mobile agent-based IDS (Fig. 10) ease the system whereby some functions are only assigned to mobile agents without burdening every nodes in the network. This is major contributing factor to reduce energy consumption in MANET whereby energy consumption is very crucial in MANET [48]. Dastjerdi et al. [49] has proposed and implemented an IDs which utilizes MA to detect intrusions in cloud environment.

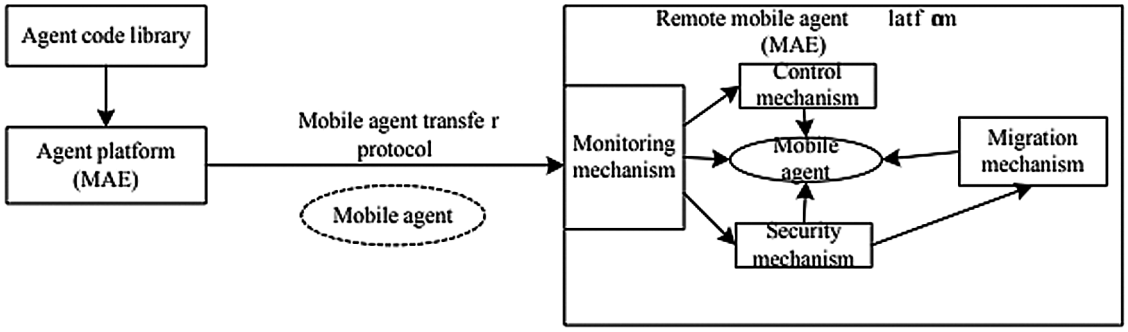

Figure 10: Mobile agents [50]

4 Design Challenges of Wireless IDS and Recommendations

One of the weaknesses of traditional wired IDS is it does not generally detect network intrusion from internal hosts of the network. Although it is possible to protect an organization internal network from wireless attackers, make sure there is only one link between the WNs and the main network, such a network IDs will not cover all of the traffic on the WN [51]. The traditional wired IDS may meet some challenge of securing the WN because it fundamentally ignores the monitoring of airspace from which most attacks are perpetrated. The wired IDS is not suitable for analyzing WN because most of the *ad hoc* network device is using a wireless connection point and connected with a WN. To further argue on that some of the problems of detecting intrusions in wireless network are Inconsistency of the strength of signal, difficulty in detecting unofficial user, interference of Radio Frequency, numerous channels, various type of protocols and location of sensors [52].

4.1 IoT Networks

The IoT connected devices in 2018 was 23.14 billion, and there are different behaviors and characteristics of network traffic on each IoT devices, so should select the devices that is commonly used by people. After that, one must collect a huge amount of data on the IoT network in order to understand the IoT network traffic behavior and the characteristic. The lack of availability of large real-world datasets for IoT has become the challenge for IDS in IoT. At last, need to select a set of algorithms for analyzing the IoT network traffic with the KDD Cup data set. Khammassi et al. [53], the author uses Genetic Algorithm (GA) to detect the various types of network intrusions by applying the standard KDD99 benchmark dataset and obtained reasonable detection rate.

Chen et al. [54] also addresses some of the constraints in the wireless such mobility, no central points, constraint in terms of the wireless link bandwidth and limited resources. These factors need to address in order to develop a comprehensive IDs mainly for wireless systems alone.

4.2 Wireless Sensor Networks (WSN)

Bridges et al. [55] has addressed some concerns and research challenges towards the IDS design in WSN in terms of communications and networking aspects. Since WSN works in the distributed nature, the author suggests ways to secure the strategies which is limited in terms of resources. One main concern is the infrastructure less nature of the WSN makes it very hard to design secured algorithms and models like routing, encryption and communications for WSN. Moreover, the limited resources of WSN nodes in terms of bandwidth, throughput and battery power also need to be taken into consideration. The nodes in WSN are subjected physical attacks such as tampering and hijacking which may affect the operations of the network. And the nature of wireless links is prone to eavesdropping attacks which can easily expose important information to adversary which may lead to DOS attacks eventually. In WSN, there is no such

thing as centralized trusted authority and any decisions made must be performed collaboratively. So, when designing IDS in WSN, this limitation have to be taken into consideration. So as a recommendation for IDS design in WSN, for mobile sensor network where nodes are always in the moving position, a distributed or cooperative IDS design is more suitable as it is robust, scalable and fast. Butun et al. [33,55,56] and Alrajeh et al. [57] proposed such IDS designs for mobile wireless sensor network. Whereas for static sensor network with centralized computing unit, a centralized IDS design is recommended as they are capable in detecting wider range of attacks. Wang et al. recommended such scheme and can be a good point to start with. As for the cluster-based network with hierarchical arrangement of cluster head nodes and cluster nodes, a hierarchical IDS design would be the most suitable. The work by Su et al. [58] is suitable if the network is steady and no nodes required to be added in the future. On the other hand, if the network is very dynamic in nature and needs to be expanded then the work by Bao et al. [59] is more suitable.

4.3 Mobil Ad Hoc *Network*

Mobile *ad hoc* networks consist of many features such as dynamic nature of topology, limited energy and improper security that makes it very complex [60]. Due to these, they are very vulnerable to attacks and various IDS have been proposed in the literature. Since the nodes in *ad hoc* are always mobile, the IDss proposed in the wired network cannot be directly applied to MANET. Moreover security in MANET is a very serious concern due to not having a fixed topology, very vulnerable media that is open and any malicious nodes can just create attacks due to hostile environment [61]. In order to consider IDS in MANET few constrains needs to be considered such as (i) very hard to perform centralized management due to unfixed infrastructure, (ii) a lot of bandwidth usage due to large numbers of nodes, (iii) the bandwidth constraint of wireless channels, (iv) false positive and false negative alarms due to the distributed nature of IDS in MANET and lastly protection of IDS in wireless itself is already a critical factor [62].

So in order to address some of these challenges, the wireless IDS should be distributed and collaborative in nature and this is proven in the work by Mohammadi et al. [63], Khan et al. [64], and Keramatpour et al. [65] follow this idea. Whereas, Kachirski et al. [66] and Daniel et al. [67] employ the alternative way variation of the distributed and collaborative architectures. This kind of distributed nature is good for detecting security incidents but requires a lot of resources and hard to be implemented in tiny devices like PDA [68].

5 Conclusion

This paper presents a survey to re-architecting IDS design to accommodate IoT and Manet characteristics. We holistically presented the review, from basic IDS deployment strategies to traffic analysis and wireless network recommendations. The overall survey gives the reader a complete understanding of what an IDS is, the data or traffic involved in detecting an anomaly, and some design challenges in adopting wired IDS design into wireless IDS. The paper's main highlight focuses on the design challenges of IDS in wireless networks such as MANET, IoT, and VANET. Based on existing research gaps, traffic headers specific to wireless networks (from 802.11 frames and data link layer) should be more heavily weighted in the network analysis. The paper concludes with several recommendations and guidelines for IDS design that are mainly effective against intrusions in the wireless space.

Funding Statement: The authors acknowledge Jouf University, Saudi Arabia for his funding support.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Z. Jhanjhi, M. Humayun and S. N. Almuayqil, "Cyber security and privacy issues in industrial internet of thing," *Computer Systems Science and Engineering*, vol. 37, no. 3, pp. 361–380, 2021.

[2] P. Wanda, "A survey of intrusion detection system," *International Journal of Informatics and Computation*, vol. 1, no. 1, pp. 1–10, 2020.

[3] A. G. Tartakovsky, B. L. Rozovskii, R. B. Blazek and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods," *IEEE Transactions on Signal Processing*, vol. 54, no. 9, pp. 3372–3382, 2006.

[4] H. J. Liao, C. H. R. Lin, Y. C. Lin and K. Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[5] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.

[6] M. Humayun, N. Z. Jhanjhi, B. Hamid and G. Ahmed, "Emerging smart logistics and transportation using IoT and blockchain," *IEEE Internet of Things Magazine*, vol. 3, pp. 58–62, 2020.

[7] S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain and M. Humayun, "Performance enhancement in wireless body area networks with secure communication," *Wireless Personal Communications*, vol. 116, no. 1, pp. 1–22, 2021.

[8] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for IoT," *IEEE Access*, vol. 8, no. 1, pp. 88892–88932, 2020.

[9] F. Zahra, N. Jhanjhi, S. N. Brohi, N. A. Malik and M. Humayun, "Proposing a hybrid RPL protocol for rank and wormhole attack mitigation using machine learning," in *Proc. ICCIS*, Saudi Arabia, AL-Jouf, KSA, pp. 1–6, 2020.

[10] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system," *Future Generation Computer Systems*, vol. 80, no. 1, pp. 157–170, 2018.

[11] M. Nooribakhsh and M. Mollamotalebi, "A review on statistical approaches for anomaly detection in DDoS attacks," *Information Security Journal: A Global Perspective*, vol. 29, no. 3, pp. 118–133, 2020.

[12] K. Siddique, Z. Akhtar, F. A. Khan and Y. Kim, "KDD Cup 99 data sets: A perspective on the role of data sets in network intrusion detection research," *Computer*, vol. 52, no. 2, pp. 41–51, 2019.

[13] Z. Ghazi and A. Doustmohammadi, "Intrusion detection in cyber-physical systems based on Petri net," *Information Technology and Control*, vol. 47, no. 2, pp. 220–235, 2018.

[14] R. Mitchell and I. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 5, pp. 1–29, 2014.

[15] R. Kumar and D. Sharma, "HyINT: Signature-anomaly intrusion detection system," in *Proc ICCCNT*. Bengaluru, India, pp. 1–7, 2018.

[16] P. Mishra, E. S. Pilli, V. Varadharajan and U. Tupakula, "Intrusion detection techniques in cloud environment: A survey," *Journal of Network and Computer Applications*, vol. 77, no. 1, pp. 18–47, 2017.

[17] A. Hussain and P. Sharma, "Efficient working of signature based intrusion detection technique in computer networks," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 12, no. 10, pp. 60–64, 2019.

[18] S. Aljawarneh, M. Aldwairi and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Journal of Computational Science*, vol. 25, no. 1, pp. 152–160, 2018.

[19] A. Karami, "An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities," *Expert Systems with Applications*, vol. 108, no. 1, pp. 36–60, 2018.

[20] A. K. Saxena, S. Sinha and P. Shukla, "General study of intrusion detection system and survey of agent based intrusion detection system," in *Proc. ICCCA*, Greater Noida, India, pp. 101701, 2017.

[21] K. Nathan, S. Y. Ji, A. Chaudhary, C. Concolato, B. Yu *et al.,* "A survey of cloud-based network intrusion detection analysis," *Human-centric Computing and Information Sciences*, vol. 6, no. 1, pp. 1–16, 2016.

[22] S. Rizvi, L. Gabriel, M. Guyan and J. Savan, "Advocating for hybrid intrusion detection prevention system and framework improvement," *Procedia Computer Science*, vol. 92, no. 1, pp. 369–374, 2016.

[23] B. S. Bhatti and C. S. Rai, "Analysis of support vector machine-based intrusion detection techniques," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 371–2383, 2020.

[24] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks*, vol. 61, no. 1, pp. 85–117, 2015.

[25] B. Shah and B. H. Trivedi, "Artificial neural network based intrusion detection system: A survey," *International Journal of Computer Applications*, vol. 39, no. 6, pp. 13–18, 2012.

[26] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun *et al.,* "Secure healthcare data aggregation and transmission in IoT-a survey," *IEEE Access*, vol. 9, no. 1, pp. 16849–16865, 2021.

[27] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on emerging topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[28] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," in *Proc. WINCOM*, Fez, Morocco, pp. 258–263, 2016.

[29] C. Yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, no. 1, pp. 21954–21961, 2017.

[30] Y. Mehmood, M. A. Shibli, U. Habiba and R. Masood, "Intrusion detection system in cloud computing: Challenges and opportunities," in *Proc. NCIA*, Rawalpindi, Pakistan, pp. 59–66, 2013.

[31] A. Luckow, M. Cook, N. Ashcraft, E. Weill, E. Djerekarov *et al.,* "Deep learning in the automotive industry: Applications and tools," in *Proc. Big Data*, Washington, DC, USA, pp. 3759–3768, 2016.

[32] M. Komar, P. Yakobchuk, V. Golovko, V. Dorosh and A. Sachenko, " Deep neural network for image recognition based on the Caffe framework," in *Proc. DSMP*, Lviv, Ukraine, pp. 21–25, 2018.

[33] I. Butun, S. D. Morgera and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2013.

[34] T. S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art," *Computer Standards & Interfaces*, vol. 28, no. 6, pp. 670–694, 2006.

[35] M. Chirag, D. Patel, B. Borisaniya, H. Patel, A. Patel *et al.,* "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[36] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," in *Proc. CCS'02*, New York, NY, United States, pp. 255–264, 2002.

[37] F. Erlacher and F. Dressler, "On high-speed flow-based intrusion detection using snort-compatible signatures," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 1, pp. 1, 2020.

[38] J. Arshad, M. Abdellatif, M. M. Khan and M. Azad, "A novel framework for collaborative intrusion detection for M2M networks," in *Proc. ICICS*, Irbid, Jordan, pp. 12–17, 2018.

[39] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for VANET," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 148–161, 2018.

[40] M. Idhammad, K. Afdel and M. Belouch, "Distributed intrusion detection system for cloud environments based on data mining techniques," *Procedia Computer Science*, vol. 127, no. 1, pp. 35–41, 2018.

[41] M. Ozalp, C. Karakuzu and A. Zengin, "Distributed intrusion detection systems: A survey," *Academic Perspective Procedia*, vol. 2, no. 3, pp. 400–407, 2019.

[42] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[43] L. Chao, B. Shanmugam, S. Azam, A. Karim, A. Islam *et al.,* "Intrusion detection system for the internet of things based on blockchain and multi-agent systems," *Electronics*, vol. 9, no. 7, pp. 1120–1130, 2020.

[44] A. Omar, M. A. Kiram, O. Bourkoukou and S. Elbouanani, "A new distributed intrusion detection system based on multi-agent system for cloud environment," *International Journal of Communication Networks and Information Security*, vol. 10, no. 3, pp. 526–528, 2018.

[45] M. R. Sanjay, "Secure cloud computing based on mutual intrusion detection system," *International Journal of Computer Application*, vol. 1, no. 2, pp. 57–67, 2012.

[46] W. Huang, Y. An and W. Du, "A multi-agent-based distributed intrusion detection system," in *Proc. ICACTE*, Chengdu, China, pp. 1–10, 2010.

[47] A. S. Rahman, H. Tout, T. Chamseddine and A. Mourad, "Internet of Things intrusion detection: Centralized, on-device, or federated learning?," *IEEE Network*, vol. 34, no. 6, pp. 310–317, 2020.

[48] A. Odesile and G. Thamilarasu, "Distributed intrusion detection using mobile agents in wireless body area networks," in *Proc. EST*. Canterbury, UK, pp. 141–149, 2017.

[49] A. V. Dastjerdi, K. A. Bakar and S. G. H. Tabatabaei, "Distributed intrusion detection in clouds using mobile agents," in *Proc. ADVCOMP*, Sliema, Malta, pp. 175–180, 2009.

[50] G. Kun and J. Sumei, "Research on the application of mobile agent in intrusion detection technology," in *Proc. ICCEA*, Bali Islnad, Indonesia, pp. v6-549, 2010.

[51] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. Rodrigues *et al.,* "Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: Survey and future challenges," *IEEE Access*, vol. 8, no. 1, pp. 3343–3363, 2019.

[52] Y. Farooq, H. Beenish and M. Fahad, "Intrusion detection system in wireless sensor networks—A comprehensive survey," in *Proc. INTELLECT*, Karachi, Pakistan, pp. 1–6, 2019.

[53] C. Khammassi and S. Krichen, "A GA-LR wrapper approach for feature selection in network intrusion detection," *Computers & Security*, vol. 70, no. 1, pp. 255–277, 2017.

[54] L. Chen, S. Zhou and J. Xu, "Computation peer offloading for energy-constrained mobile edge computing in small-cell network," *IEEE/ACM Transactions on Networking*, vol. 26, no. 4, pp. 1619–1632, 2018.

[55] R. Bridges, G. Vanderlan, T. R. Iannacone, M. D. Vincent, MS *et al.,* " A survey of intrusion detection systems leveraging host data," *ACM Computing Surveys (CSUR)*, vol. 52, no. 6, pp. 1–35, 2019.

[56] D. Silva, A. R. Paula, M. H. Martins, B. Rocha, A. Loureiro *et al.,* "Decentralized intrusion detection in wireless sensor networks," in *Proc. Q2SWinet '05*, New York, NY, United States, pp. 16–23, 2005.

[57] N. A. Alrajeh, S. Khan and B. Shams, "Intrusion detection systems in wireless sensor networks: A review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, pp. 167575, 2013.

[58] C. Chung Su, K. M. Chang, Y. H. Kuo and M. F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks [wireless sensor networks]," in *Proc. WCNC*, New Orleans, LA, USA, pp. 1927–1932, 2005.

[59] F. Bao, R. Chen, M. Chang and J. H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[60] P. Yi, Z. Dai, S. Zhang and Y. Zhong, "A new routing attack in mobile ad hoc networks," *International Journal of Information Technology*, vol. 11, no. 2, pp. 83–94, 2005.

[61] S. Shahzadi, F. Ahmad, A. Basharat, M. Alruwaili, S. Alanazi *et al.,* "Machine learning empowered security management and quality of service provision in SDN-NFV environment," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2723–2749, 2021.

[62] M. Mohammadi, T. A. Rashid, S. H. Karim, A. Hussain, M. Aldalwie *et al.,* "A comprehensive survey and taxonomy of the SVM-based intrusion detection systems," *Journal of Network and Computer Applications*, vol. 178, no. 1, pp. 102983–103007, 2021.

[63] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal *et al.,* "A survey on intrusion detection and prevention in wireless ad-hoc networks," *Journal of Systems Architecture*, vol. 105, no. 1, pp. 101701–101718, 2020.

[64] A. Keramatpour, A. Nikanjam and H. Ghaffarian, "Deployment of wireless intrusion detection systems to provide the most possible coverage in wireless sensor networks without infrastructures," *Wireless Personal Communications*, vol. 96, no. 3, pp. 3965–3978, 2017.

[65] B. Sun, K. Wu and U. W. Pooch, "Alert aggregation in mobile ad hoc networks," in *Proc. WiseML '20*, Ney York, NY, United States, pp. 69–78, 2003.

[66] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks," in *Proc. HICSS'03, NW*, Washington, DC, United States, pp. 8–15, 2003.

[67] S. Daniel, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade *et al.,* "A general cooperative intrusion detection architecture for MANETs," in *Proc. IWIA'05*, College Park, Maryland, pp. 57–70, 2005.

[68] S. Mandala, M. A. Ngadi and A. H. Abdullah, "A survey on MANET intrusion detection," *International Journal of Computer Science and Security*, vol. 2, no. 1, pp. 1–11, 2007.