IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 21, 2017, accepted January 2, 2018, date of publication January 23, 2018, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2793841

Denial of Service Defence for Resource Availability in Wireless Sensor Networks

OPEYEMI A. OSANAIYE[1], ATTAHIRU S. ALFA[1,2], (Member, IEEE), AND GERHARD P. HANCKE[1], (Fellow, IEEE)

[1]Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa
[2]Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, MB R3T 2N2, Canada

Corresponding Author: Opeyemi A. Osanaiye (opyosa001@myuct.ac.za)

This work was supported by the Advanced Sensor Networks SARChI Chair Program, co-hosted by the University of Pretoria and the Council for Scientific and Industrial Research, through the National Research Foundation of South Africa.

ABSTRACT Wireless sensor networks (WSN) over the years have become one of the most promising networking solutions with exciting new applications for the near future. Its deployment has been enhanced by its small, inexpensive, and smart sensor nodes, which are easily deployed, depending on its application and coverage area. Common applications include its use for military operations, monitoring environmental conditions (such as volcano detection, agriculture, and management), distributed control systems, healthcare, and the detection of radioactive sources. Notwithstanding its promising attributes, security in WSN is a big challenge and remains an ongoing research trend. Deployed sensor nodes are vulnerable to various security attacks due to its architecture, hostile deployment location, and insecure routing protocol. Furthermore, the sensor nodes in WSNs are characterized by their resource constraints, such as, limited energy, low bandwidth, short communication range, limited processing, and storage capacity, which have made the sensor nodes an easy target. Therefore, in this paper, we present a review of denial of service attacks that affect resource availability in WSN and their countermeasure by presenting a taxonomy. Future research directions and open research issues are also discussed.

INDEX TERMS Denial of service (DoS), detection techniques, intrusion detection system (IDS), resource availability, resource depletion, wireless sensor networks (WSNs).

I. INTRODUCTION

Advancement in wireless communication and electronics over the years has led to the development of wireless sensor networks (WSNs). WSNs are formed by sets of distributed autonomous devices with several distinct characteristics to sense, process, transmit and receive observed or measured condition. Its deployment has been enhanced by its small, inexpensive and smart sensor which is easily deployable. In its simplest form, the sensor node is made up of a sensor component that measures the condition of the observed situation or physical surrounding of interest while the microprocessor component of the node ensures the information obtained are intelligently computed [1]. The wireless radio embedded in the nodes allow communication between the neighbouring nodes. A considerable number of these sensors are used to cover the area of interest since a single sensor node can only provide limited information.

WSN are often deployed in remote, hearse and unattended environment over a specified period, to transmit information that can be accessed and interpreted by an end user. Often a times, the locations where sensor nodes are deployed are not accessible, therefore, it is impractical to carry out regular maintenance on the nodes after installation. WSNs in recent times are gaining popularity due to the fact that they are economically viable solutions to a cross section of real-world challenges [2]. Its wide range of applications cut across periodic monitoring, target tracking, query-based and event-driven applications [3]. Its monitoring application can be harnessed during ubiquitous monitoring and health monitoring such as monitoring the patient's temperature, heart beat rates, blood pressure and other health related issues to take appropriate steps in the case of any health problem. Furthermore, it can be applied in the area of environmental surveillance for detecting oil spillage and quality of air. WSNs can also be used for industrial applications such as pipeline monitoring, smart grid monitoring and precision agriculture for agricultural farm management [3]. Other common application includes its use for military

operations, distributed control system and detection of radioactive sources.

WSN has become one of the most preferred networking solutions, however, it's extremely limited resources such as energy, memory, computing and bandwidth has made it vulnerable to both passive and active attack. Passive attack is carried out by an adversary by monitoring an ongoing communication between two nodes (e.g. eavesdropping) [4] while an active attack takes advantage of the broadcast nature of wireless communication medium to launch an attack. Furthermore, sensor nodes are exposed to physical attacks as a result of its lack of tamper-resistance due to cost constraint. Common among the security threats in WSN are denial of service attack, communication attack, node compromise, protocol-specific attack and impersonation attack [5].

The network security policy is guided by the confidentiality, integrity and availability (CIA) triad model [6]. Both the integrity and confidentiality of transmitted data in WSN have attracted the attention of security experts, both in the academia and industry, while not much interest has been given to security attacks that affects the availability of resources. Resource depletion attacks primary aim is to exhaust the limited resources in WSN to the detriment of its existence and functionality, which can lead to the outage of sensor nodes. Therefore, maintaining high availability is a major task in the design and deployment of WSN. An example of resource depletion attack is the denial of service (DoS) attack, its distributed form, DDoS and Jamming attack that affects the long-term availability of sensor nodes by depleting the nodes battery life to cause a permanent shutdown.

In this paper, we review the different forms of DoS attacks that depletes the resources of sensor nodes in WSN. Furthermore, we discuss the various mitigation techniques that have been proposed in the literature and their deployment location. Unlike other wireless networks, WSN is characterised by resource limitation, therefore proposed mitigation techniques must be efficient and lightweight to ensure a high detection rate and low false alarm.

This paper presents an extensive review of DoS attacks and its countermeasures in WSNs between 2002 and 2017. A small number of reviews have been published on security in WSNs, however, our survey differs from previous surveys in the following ways:

(i) Wood and Stankovic [7], for example, presents a taxonomy for DoS attacks and possible defence measures, whilst we focus on a more recent and holistic approach to DoS attacks, defence and deployment location.

(ii) Zhang *et al.* [121] presented a survey on outlier detection techniques in WSN that includes noise and error, events and malicious attacks, whilst we focus specifically on DoS attack that drains the energy and deplete the resources of the deployed sensor nodes.

(iii) Abduvaliyev *et al.* [8], Butun *et al.* [9] and Xie *et al.* [5] presented a general review of anomaly detection in WSNs, however, in our work, we focus mainly on DoS attacks that aim to deplete the energy and resources of the deployed sensor nodes and its defences.

(iv) Vadlamani *et al.* [38] in their work presented a taxonomic survey of jamming attacks in wireless networks, however in our work, in addition to jamming attack, we present other DoS attacks targeting different layers of the WSN and their defence solutions.

The rest of the paper is organized as follows. Section II presents an overview of WSNs and its architecture while Section III discusses security requirements in WSN. Resource exhaustion attacks in WSN caused by DoS attack is discussed in Section IV while Section V highlights proposed DoS defences by presenting a taxonomy. Section VI presents a general discussion and drawbacks on existing proposed techniques. Finally, Section VII concludes the paper and presents some future open research.

II. WSN ARCHITECTURE

Conventionally, WSNs consist of tens of thousands of sensor nodes that communicate between member nodes. It first of all sense information of interest before using an inbuilt microcontroller to process the sensed information. Thereafter, it communicate the result to a base station without an existing infrastructure [10]. The limitation of a single sensor node has necessitated a network of sensor nodes that are self-organising. They collaborate with one another to provide coverage over a large environment to achieve a common task. Routing protocols in WSNs coordinate how sensor nodes communicate with each other by ensuring that the most optimal route is transverse when conveying sensed information towards the base station. Ogundile and Alfa [11] in their work present a state-of-the-art survey on energy-efficient and energy-balanced routing protocols for WSN. One of the most significant benefits of the sensor network is its ability to extend its computation capability to physical environment, where access by human beings is almost impossible.

WSNs can be categorized according to the environment which it is being deployed. Yick *et al.* [12] described five types of WSNs, namely: terrestrial WSN, underground WSN, underwater WSN, mobile WSN and multi-media WSN.

- Terrestrial WSNs: In terrestrial WSNs, hundreds to several thousands of cheap sensor nodes are deployed within a specific area as either an ad hoc or a pre-planned deployment. In an ad hoc deployment, these sensor nodes can be dropped from a plane and randomly deployed on the target area while examples of pre-planned deployment are grid placement, optimal placement, 2-D and 3-D placement models [13].
- Underground WSNs: Underground WSNs are sensor nodes concealed under the ground to monitor its condition. In this deployment, sink nodes are placed above the ground to relay transmitted sensor readings from the sensor nodes to the base station [14]. When compared with terrestrial WSN, underground WSN is more expensive as regards to equipment, deployment and maintenance.

- Underwater WSNs: Underwater WSNs are sensor nodes and vehicles deployed beneath the surface of the water, for exploration or gathering of data to transmit acoustic waves [15]. The sensor nodes used here are fewer and more expensive than the terrestrial WSNs. In addition, underwater WSN deployment of sensor nodes is sparse as compared to the dense deployment of terrestrial WSN.
- Mobile WSNs: A group of sensor nodes that move and interact with the physical environment is referred to as Mobile WSNs. Just as in the case of static nodes, mobile nodes have the potential to sense, process, transmit and receive measured or observed conditions. After deployment, mobile nodes can reorganize and reposition themselves in the network to gather information. The information gathered can be distributed to other mobile nodes within their communication range. One of the key difference between mobile and static WSN is that the latter uses a dynamic routing protocol to distribute information while the former uses flooding or fixed routing protocol [12].
- Multi-media WSNs: The last type of WSN, multi-media WSN, has been proposed. These are low cost sensor nodes equipped with microphones and cameras to enable the tracking and monitoring of multi-media related events in the form of audio, video and imaging [16]. The multi-media sensor nodes function by interconnecting with each other over a wireless medium to retrieve, compute, compress and transmit data in a pre-planned arrangement to ensure coverage. The deployment of multi-media sensor nodes is often faced with resource challenges; among which are excessive energy consumption, high bandwidth demand, ensuring quality of service, compression and decompression techniques.

The structure of WSN can be classified according to the uniformity of the deployed sensor nodes. Some of these deployments are made up of uniform nodes with equal capacity while others make distinctions in the nodes, depending on their architecture. There are three main types of network topology (structure) in WSNs; Flat-based (tree), cluster-based and hierarchical [8].

- Flat-based topology: In this topology, all the nodes deployed in the network plays the same role i.e. sensing the event, processing the information, transmitting the data through multi-hop routing and reporting the event [17] – see Fig.1. Flat topology architecture has been used by data aggregation protocols, data gathering protocols, routing protocols and node scheduling protocols [18]. This topology uses quality routes to transmit data from the source node to the sink node by flooding. Flooding is a technique where a node broadcast information and control packets which it has received to the other nodes in the network. This process is repeated until the destination node is reached. Data aggregation is achieved in a flat network by data-centric routing, where the base station broadcast a query message to the sensor nodes by flooding. The sensor nodes that have the matching data in the query, thereafter sends a response back to the base station [18]

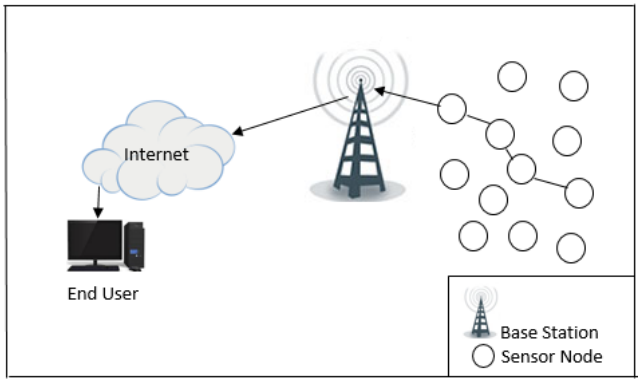

FIGURE 1. Flat-based WSN topology.

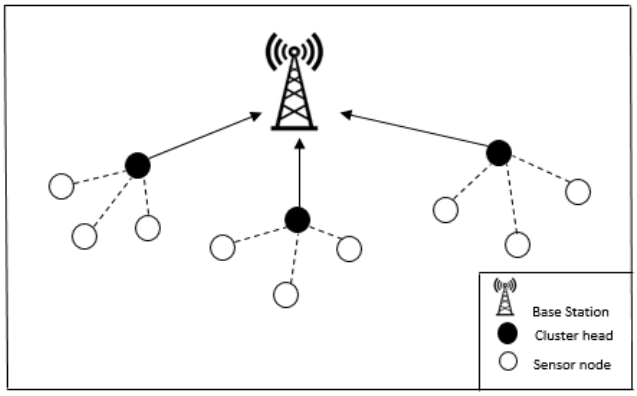

FIGURE 2. Cluster-based WSN topology.

- Cluster-based topology: This structure is formed in WSN by grouping the nodes into three main elements; the sensor nodes, the cluster heads and the base station (- see Fig. 2). The sensor nodes are set of nodes in the network that monitor and sense the environment to collect data of interest. These nodes are arranged in clusters and transmits the sensed data to the cluster head after processing. Every cluster formed selects a cluster head that serves as a bridge between its cluster members and the base station. The cluster head functions by performing tasks like data aggregation, for all nodes in the cluster, before sending it to the BS. This way, the cluster heads serves as a sink to other member nodes and the BS serves as a sink to the cluster heads. In some cases, the cluster heads are allowed to communicate with themselves [8]. The cluster-based topology can be classified as either homogeneous or heterogeneous and static or dynamic clusters. It can be replicated throughout the network, creating different layers of the hierarchical-based WSN [18].
- Hierarchical-based topology: Hierarchical architecture was design to distribute sensing and processing tasks

into different level of the system. The network is arranged in a tree-like structure with different types of cluster [8]. Yick *et al.* [12] described four tiers of the hierarchical architecture, namely: sensor-level, node-level, group-level, and base-level. The sensor level is the lowest level, comprising of individual sensors with sensing algorithm that detects and classify objects. After processing the sensed data, the sensing algorithm sends the classification result to the node-level. Here, classification deals with the fusion of the sensed data obtained from each node. The sensor-level and the node-level both reside in the node. The group-level is formed by set of nodes that are organised in groups with an elected group leader to perform group-level classification. The aggregated attribute result of the node-level classification is the input to the group-level classification, where group leaders (i.e. cluster heads) can achieve advanced tasks. The base-level classification is the highest level that receives results from the group-level classification and transmits it to the base station via multi-hop. The base-level classification algorithm finalizes the collected results and reduces false alarm among the results reported.

III. SECURITY REQUIREMENTS IN WSNs

The security requirements in WSNs are novel, when compared to other wireless communication medium, due to its resource constraints, architecture and deployment area. Security is critical to many applications of sensor networks and is often guided by the security triad model; confidentiality, integrity and availability (CIA). Mission critical applications [19] like healthcare and military applications convey real-time and sensitive information which requires continuous service to enhance the decision-making process. The consequence of interruption or access to the flow of information (e.g. life support monitoring or enemy tracking) will be catastrophic, therefore, adequate protection of the resources and information transmitted over the network must be guaranteed.

- Confidentiality: Confidentiality in WSNs entails the assurance that sensitive information is well protected and not accessible to unauthorized persons while in process, transit or storage. Sensitive information like military information, health condition and industrial secrets must not be understood by anyone except the intended recipients. While confidentiality in WSNs in very important, it is not applicable in cases where sensed and monitored information is of public use (e.g. temperature of a city). One of the prominent attacks against the confidentiality of the sensor nodes, eavesdropping attack, can be mitigated by deploying secret sharing cryptography [20]. Encryption of data [21], [22], authorization and key distribution mechanism [23] have also been suggested in the literature as countermeasures against confidentiality attack in WSN.

  All these proposed mitigation solutions for preserving the confidentiality of the transmitted information in WSN must be specially designed for resource constrained sensor nodes. This is necessary as most proposed solutions consume excessive energy during the encryption and decryption process of encoding and decoding transmitted information.
- Integrity: The integrity of information sensed, processed, transmitted and stored by sensor nodes must be protected against unauthorized falsification, modification and deletion. As wireless channels can be accessed by anyone, it is prone to unauthorized access which can lead to data manipulation. An example of such attack is the false data injection attack [24]. Furthermore, attenuation and data loss, due to harsh weather condition and unreliable communication channel, can alter data without the influence of an intruder [25]. The implementation of WSN will fail to achieve its purpose if inaccurate data is received; which will in turn affect the decision made by the end user. Therefore, providing data integrity in wireless communication medium is not just enough countermeasure. Compromised sensor nodes can still listen to transmitted messages, which can be replayed later to disrupt data aggregation result. Cyclic codes and message authentication codes are often used to protect data integrity in WSNs [26]. Just as in the case of attacks on the confidentiality of information in WSN, mitigation solutions for integrity attack must also be specially suited to sensor nodes.
- Availability: When determining availability in WSN, security, infrastructural failure, application failure and energy depletion are the four main factors to be considered. Availability in WSN guarantees that services, resources and information are accessible to authorized users when requested. This means a reliable service will be provided by the network, by ensuring that data is delivered to the intended destination, even during the instance of an attack threat [20]. Maintaining a high availability has become a major task in the design and deployment of WSN because of its extremely limited resources (i.e. limited energy, memory, computing and bandwidth). The limited resources in WSN has made it a soft target to various resource exhaustion attacks. The availability fault, therefore, become less tolerable as it is pivotal to its existence. Closely related to availability is resilient and self-healing requirement [20]. This ensures that senor nodes in WSN recover from security attacks by isolating the source of the threat to stop future attacks on the availability of resources and services. An example of such attack is the DoS attack that depletes the resources of sensor nodes to ensure they do not carry out their intended functions, by draining the available energy which in turn affects their long-term availability. Intrusion detection system has also been proposed to protect the sensor nodes infrastructure, resource and service [27], [28].

From the security triad model mentioned above, the main focus of this work is the DoS attacks that affect the

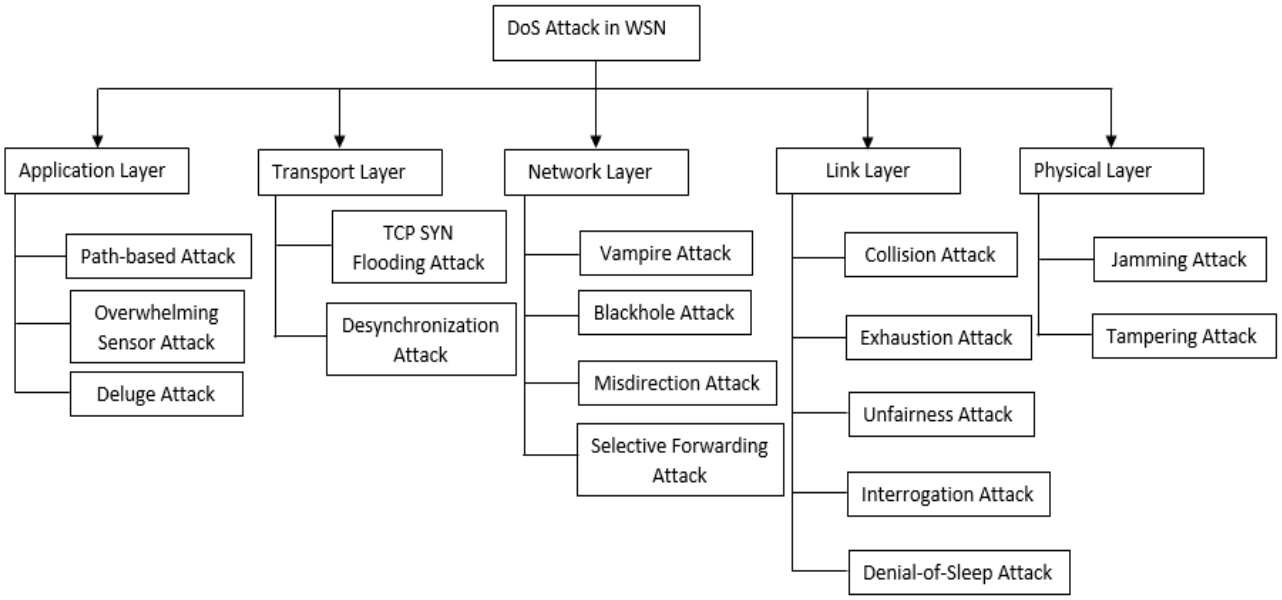

FIGURE 3. DoS attack taxonomy in WSN.

availability of services and resources in WSNs and its countermeasures. The requirements of availability are placed at a higher rank when compared with confidentiality and integrity because if sensor nodes are disabled, they cannot function; therefore, any other security measure configured is null and void.

IV. RESOURCE EXHAUSTION ATTACKS IN WSNs

Resource exhaustion or depletion attack is any intentional activity that aims to subvert, disrupt or bring down part or the entire network, to achieve functionality degradation, thus compromising the availability of the system. Most of this type of attack target the vulnerability of the system; hence, in WSNs, the limited energy, memory and processing capability has been the target of one of such attack, DoS attack [23], [28]. DoS attack is a major threat to the existence of WSN due to the ease at which it can be perpetrated. In its simplest form, DoS can be carried out by compromising either internal or external vulnerable nodes. In an internal attack, the adversary compromises the internal node remotely by sending series of malformed packets towards the target node, to overwhelm and consume its resources before eventually shutting it down [29]. During an external attack, the cluster heads are often the target.

Different forms of DoS attacks that target different layers of the WSN have been reported. Shu *et al.* [30] describe how DoS attacks can be used to disrupt normal traffic delivery between the sensor node and the sink node, to generate blackholes. A blackhole is accomplished when an adversary passively intercepts or actively block the delivery of information. An attack on routing protocols, Vampire attack, was described by Vasserman and Hopper [31]. Vampire is a DoS attack that does not immediately disrupt the availability of the network, but function by draining life out of the sensor nodes over time. Vampire attacks are not protocol specific and do not rely on protocol vulnerability, but rather exploits the general features of protocol classes. Gill and Yang [32] identified two categories of DoS attack in WSN; the one that exploits the vulnerability of the network and the other that does not. When the former is exploited, attackers establish limited number of connections to the victim node and sends low volume of specially crafted packets while the latter uses a less intelligent but effective technique like the flooding attack.

DoS Attack in WSNs: A DoS attack in WSN exists in different forms, and can target sensor components at different layers of the WSN. Therefore, in describing DoS in WSN, we present a taxonomy of different forms of DoS attacks on layers of the sensor networks (i.e. physical, link, network, transport and application layers) – see Fig.3

A. PHYSICAL LAYER

In WSN, the physical layer is responsible for carrying out functions, such as, carrier frequency generation, frequency selection, signal detection, modulation and data encryption [23]. This shows that the function of the physical layer is delicate to the existence of WSN. The broadcast nature of wireless communication has exposed the sensor nodes to DoS attacks, that tends to jam or intercept radio signals, to disrupt the services of the sensor nodes. Additionally, nodes in WSN are often deployed in a remote, hostile and insecure environment; therefore, an attacker can have physical access to it. The two main types of DoS attacks on the physical layer are jamming and tampering attacks.

1) JAMMING ATTACK

Jamming can be described as the disruption of transmitted wireless signal. This can occur either intentionally

(radio frequency interference) or unintentionally, in the form of noise, interference or collision at the receiver, or in the context of an attack [33]. The objective of jamming attack is to prevent devices from communicating by using as little power as possible. Jamming attacks exploit the shared nature of the wireless medium to disrupt communication, by reducing the signal to noise ratio (SNR). An attacker with enormous resources can regularly jam the spectrum band, to ensure that communication in the band is interrupted. Furthermore, the attacker can intermittently jam, forcing the receiver to drop packets as a result of alteration [34]. The jamming device used in carrying out this attack choses a common channel, which the nodes are using, to block data from successful transmission. The main objective of the jamming device is to ensure that the network is not available for the node to use, while the nodes, on the other hand, tries to maximize the use of the network.

The key point in carrying out a successful jamming attack is the SNR. SNR $= P_{signal}/P_{noise}$, where P is the average power. Noise here is the undesirable accidental fluctuations of electromagnetic spectrum from the antenna. Jamming attack is considered effective if SNR < 1. Santoro *et al.* [35] discussed two types of jamming attacks, the physical and the virtual jamming. Examples of physical jamming attacks are radio jamming and collision attack while network allocation vector attacks and Request-To-Send/Clear-To-Sends attacks are examples of virtual jamming attack. Khatua and Misra [36] also described the effects of jamming attack on underwater sensor networks, while a study into controllable jamming attacks on WSNs was presented in [33]. In [37], mobile jamming attack that are dynamic and can directly jam critical path of WSN was discussed. From the literature, four jamming strategies has been identified, namely: constant jammer, deceptive jammer, random jammer and reactive jammer [38], [39]. Here, we briefly discuss these strategies.

Constant jammer: In constant jammer attack, radio signal, electromagnetic waves or random sequence of bits are continually emitted to interfere with legitimate transmitted signals in the network. A constant jammer continuously sends out these random bits to occupy the transmission channel of legitimate network, thereby disallowing legitimate transmission. Additionally, it can cause an interference at the transmitting node to corrupt the signal received by the receiver. The main disadvantage of constant jammer is its enormous energy consumption, as the continuous emission of signals tends to drain energy fast, thereby requiring a high amount of power.

Deceptive jammer: Like the constant jammer attack, deceptive jammer continuously injects regular signals into the channel without gaps in between the signal. However, unlike continuous jammer, it does not emit random bits but legitimate bit sequence. This deceives the network into believing that there is a normal transmission from a legitimate node, thereby resulting in the legitimate node waiting indiscriminately in the receive state. Supposing the node has signals to transmit, it cannot change to send state because of the presence of a constant steam of incoming signals. A major advantage of deceptive jammer attack over continuous jammer is its impersonation feature which makes it more effective.

Random jammer: Random jammer attack conserve its energy by alternating between jamming and sleep state, unlike both constant and deceptive jammers. It functions by jamming for a predetermined time before turning off its radio and switching to sleep mode. After a while, it resumes back from sleeping mode to jamming mode and continue to follow that sequence. During the jamming mode, it can behave like either the constant or deceptive jammer while during the sleep mode, it does not use energy, therefore reducing power consumption.

Reactive jammer: All the three jamming strategies discussed thus far are active jammers, as they attempt to block the channel, regardless of the traffic pattern. An alternative approach to active jamming is the reactive strategy. Reactive jammer continually senses the channel to detect when signals are being transmitted. On detecting the presence of data transfer on the channel, it starts to transmit radio signals to cause collision. Reactive jammer is difficult to detect and minimises power consumption. The power it uses to listen to a channel is less than the power needed for jamming.

2) TAMPERING ATTACK

Tampering is another DoS attack in the physical layer which is primarily due to the attacker's access to the node. It targets the hardware components of the sensor nodes, such as sensitive chips and microcontrollers [8], to destroy it and cause gaps in sensor or communication coverage. Three categories of tampering attacks on microcontroller has been described in [40], namely: invasive, semi-invasive and non-invasive. Invasive attack needs access to the internals of the chip to prepare it before the attack can begin. Invasive attack often a times use expensive equipment, such as the one used for producing and testing semi-conductor. Semi-invasive, on the other hand, use a cheaper equipment and less time when compared to invasive attacks. Finally, the non-evasive attacks are the easiest to carry out [41].

B. LINK LAYER

The link layer in WSNs performs function like multiplexing of data-streams, medium access control, data frame detection and error control [23]. It ensures a reliable point-to-point and point-to-multipoint connections in the communication network. Most of the protocols that exist in the link layer cooperate to agree on channel selection and other parameters [34] which makes it vulnerable to DoS attacks. DoS attacks directed towards this layer exhaust resources and creates collision to cause unfairness in resource allocation. The main DoS attacks on the link layer are collision attack, unfairness attack, interrogation attack and denial of sleep attack [42].

1) COLLISON ATTACK

In sensor networks, collision takes place when two or more nodes transmits signals on the same medium at the same time. When signals collide, they are discarded and will require a retransmission, depending on the type of data. An attacker can intentionally fiddle with the ACK control message of the data, to cause collision [23]. This will eventually lead to a costly exponential back-off, as the attacker has violated the communication protocol by continuing to transmit data in an attempt to cause collision. A collision attack is synonymous to the reactive jamming attack because the attack is launched when the transmission of signal is sensed.

2) EXHAUSTION ATTACK

The link layer function by attempting to retransmit lost data repeatedly, even when triggered by an unusual late collision, such as those directed close to the end of the frame [43]. This type of DoS attack causes the battery resources of the nearby node to drain and exhaust, thereby compromising the availability of the sensor nodes resource, even after the attack has taken place.

3) UNFAIRNESS ATTACK

This attack in sensor networks tends to abuse the cooperative MAC layer priority scheme to cause unfairness, a form of weaker DoS attack [43]. This type of DoS attack may not totally prevent legitimate access into the channel but can create unnecessary delay in access, for real-time MAC protocols, thereby degrading it.

4) INTERROGATION ATTACK

Interrogation attacks in WSNs are DoS attacks that take advantage of the two way request-to-send/clear-to-send (RTS/CTS) handshake of the MAC protocol, used in solving the problem of hidden terminals [34]. A typical scenario of this type of attack is when a sensor node wants to transmit data, it sends a RTS frame. The receiver, upon receiving this, replies with a CTS frame, therefore all other nodes within the network that subsequently receives RTS or CTS frame desist from sending data for a particular period. An interrogation attack is carried out by continually sending RTS frames to determine the CTS response frames of the targeted receiver node. Considering the fact that the nodes are constantly preoccupied with sending CTS frames, they cannot switch into sleep mode. This will, thereafter lead to exhaustion of the available resources (i.e. energy and bandwidth) of the targeted node.

5) DENIAL-OF-SLEEP ATTACK

Access to the physical medium is coordinated by the link layer which can either be schedule based or contention based, depending on the type of application [21]. The characteristic communication pattern of the MAC protocol has made it easily susceptible to attacks, such as the denial-of-sleep attack. The denial-of-sleep is another type of DoS attack on the link layer that targets the device's power supply (battery power) [44], in an attempt to exhaust it, by preventing the radio from going to sleep mode. If many critical nodes are targeted in the network, the lifespan of the network will be reduced drastically. The link layer is often the target of denial of sleep attack because it controls the radio of a sensor node [34]. The radio component of the sensor node consumes the most energy, therefore, the MAC protocol controls the functions of the radio, such as when to transmit signals, when to listen to the channel and when to sleep. Most protocols in WSNs are designed to conserve energy, by putting the radio in sleep mode, when not in use. Some of these energy efficient MAC protocols, however, can be vulnerable to the denial of sleep attack. Bhattasali *et al.* [45] described a similar attack, sleep deprivation attack that maximizes the power consumed by the sensor nodes to minimize their life time. Denial of Sleep can be achieved through numerous ways, including the traditional DoS attack methods.

C. NETWORK LAYER

WSNs are made up of numerous sensor nodes without a pre-existing infrastructure. This, therefore means that most of the sensor nodes will serve as routers during packet transmission [43]. Since all these nodes are potential routers, it adds to the vulnerability problem of the WSNs which can be exploited by an adversary to deplete resources.

DoS attack in the network layer targets the routing protocols to manipulate it. By attacking the routing protocols, attackers can absorb the network traffic by inserting themselves in between the sending and the receiving node to control the flow of network traffic [46]. This traffic can be either routed through a non-optimal path to introduce delay, selectively or totally dropped to achieve a denial of service. Furthermore, attackers can also create routing loops to introduce severe network congestion and prevent source node packets from finding its route to the receiver. This triggers excessive network control traffic that consume resources and degrade network performance. DoS attacks in the network layer includes Vampire attack, blackhole attack, spoofing attack, replaying attack and manipulating attack.

1) VAMPIRE ATTACK

Vampire attack is a DoS attack on the network layer of WSNs. This attack crafts and transmit little chunks of malicious data to consume enormous energy when compared with a legitimate transmission in sensor networks. The resultant effect of this attack is the depletion of energy at each sensor node, which depletes the battery power. A key feature of Vampire attack is that it is not protocol specific, in that they do not rely on the design features or implementation faults of routing protocols. Vampire attack exploit the general features of protocol classes such as distant vector, link state, source routing, and geographical and beacon routing [31]. The strength of Vampire attack can be measured by the ratio of the energy used in a normal situation to the energy used during the attack.

A ratio of 1 indicates the network is safe from Vampire attack. Vampire attacks are very difficult to detect as it evades most rate limiting solutions.

2) BLACKHOLE ATTACK

Blackhole attack in WSNs is a DoS attack where a malicious node advertises itself as either the destination or the shortest path to the destination. As this advertisement propagates, the network directs more traffic towards the malicious node to cause resource contention, as neighbours deplete their resources when handling heavy traffic [43]. When the malicious node receives these packets from the other nodes, the attacker discards the packets selectively or fully. Baadache and Belmehdi [47] described two types of blackhole attack model, simple blackhole and cooperative blackhole attacks. The former is carried out when the node that serves as the dropper acts individually to carry out the attack while the latter is perpetrated using multiple blackhole nodes, that act in coordination to manipulate either the routing protocol specification or the deployed security mechanism. Furthermore, Gao *et al.* [48] in their work, also described two types of blackhole attack, namely: passive and active blackhole attacks. The passive blackhole drops all packet that passes through it without injecting false information into the network while the active blackhole attacks in addition to dropping packets also disrupts normal communication that affects the network load. A typical scenario of a blackhole attack in distance vector based (e.g. AODV) protocol involve two routing packets, RREQ (Route Request Packet) and RREP (Route Reply Packet). The RREQ, which contains the destination addresses of all the nodes in the network, is broadcasted. Upon receiving the RREQ with its address, a node in the network directly responds to the original sender with a RREP. During a blackhole attack, after receiving a RREQ, a malicious node immediately replies RREP to the source node claiming to have the shortest route to the destination. By doing this, the adversary attracts more data packets from other nodes and the source is likely to receive this false RREP emanating from the blackhole before the correct RREP packet. The source would therefore commence with the sending of data packet, after selecting the first RREP packet and dropping subsequent RREP packet received. These packets, thereafter get dropped and are never received at the destination.

3) SELECTIVE FORWARDING ATTACK

Selective forwarding attack is a derivate of blackhole attack. This attack consists of malicious nodes that may refuse to forward certain packets and simply drop them, thus causing a denial of service to legitimate packets. The adversary can evade detection by discarding from a targeted node while packets from other nodes are forwarded [49]. Selective forwarding attack is most effective when the attacker is on the data flow and can affect a number of multi-hop routing protocols.

4) MISDIRECTION

Misdirection attack in WSNs is a deliberate attempt to change, spoof or replay the routing information. This involves the forwarding of data along the wrong path or sending out a false routing update. Misdirection attack is directed towards the source of the traffic to divert it towards a predetermined destination [50]. Directing traffic towards a particular direction results in resource depletion of sensor nodes along the path. An instance of misdirection attack in WSN is the smurf attack, where an attacker forges the victim node's address as the source of many broadcast Internet Control Message Protocol (ICMP) echo. The responses to the ICMP echo packet results in the victim's node and network link being overwhelmed by excessive packets.

D. TRANSPORT LAYER

The transport layer is responsible for the end-to-end connection between the sending and receiving sensor nodes. The protocols in this layer can provide a simple unreliable area-to-area anycast, or a complex and costly reliable sequenced-multicast byte stream [43]. Most sensor network deployments, due to their resource constraints, utilize simple protocols to reduce the overheads of retransmissions and acknowledgments. Protocols with sequencing are often vulnerable to DoS attack. TCP SYN flooding and desynchronization are the two major transport layer DoS attack in WSN.

1) TCP SYN FLOODING ATTACK

The primary aim of flooding attack is to exhaust resources, such as energy, bandwidth and memory to shut it down and deny access. A classic example of flooding attack in WSN is the TCP SYN flooding attack. TCP is a connection oriented protocol that provides a reliable connection during transmission, by sending an acknowledgement message for every packet that is successfully delivered from source to destination. Before transmission, TCP does the 3-way handshaking, by first sending a SYN packet from the source to the destination node. The destination node returns a SYN+ ACK control packet as an acknowledgement, before the source finally sends an ACK to complete the 3-way handshaking process. The attacker exploits this connection orientation feature of TCP by initiating several half open connections, to occupy the link until there is a TCP connection timeout [51]. This depletes the WSN resources and deny legitimate traffic from being transmitted, thereby leading to a denial of service.

Limiting the number of concurrent connections to the target node will prevent a total exhaustion of resources, however, legitimate connections to the target node will also be affected.

2) DESYNCHRONIZATION ATTACK

Desynchronization attack in sensor network is perpetrated when the connection between the transmitting two end-point nodes is disrupted [50]. In this attack, the adversary continuously alters transmitted messages to one or both end-point nodes. This message contains sequence number and

TABLE 1. Comparative summary of DoS attacks in WSN.

Year	Reference	WSN DoS Layered Attack				
		Application	Transport	Network	Link	Physical
2002	[43]		✓	✓	✓	
2006	[39]					✓
	[41]					✓
2007	[37]					✓
	[52]	✓				
2008	[40]					✓
	[42]	✓			✓	
2009	[44]				✓	
2010	[23]				✓	
	[33]					✓
	[34]				✓	✓
	[47]			✓		
2012	[21]				✓	
	[45]				✓	
	[46]			✓		
2013	[8]					✓
	[31]			✓		
	[49]			✓		
	[50]		✓	✓		
2014	[36]					✓
	[48]			✓		
2016	[38]					✓
2017	[35]					✓

control flags that can cause the end-point nodes to request for a retransmission of corrupted or missed frames. If a proper timing is maintained by the adversary, it can hinder the end-point nodes from exchanging any meaningful information, thereby wasting energy in an infinite synchronization recovery process [43].

E. APPLICATION LAYER

In WSNs, the sensor nodes are intended to be deployed in remote unattended environments, where the sensor nodes are exposed to various attacks, such as the DoS attack. In the application layer, an adversary can overwhelm the sensor nodes with sensor stimuli [42], thereby resulting into the network sending large volume of traffic towards the base station. Attacks on the application layer consumes network bandwidth and depletes the sensor nodes energy. Path-based attack, overwhelming sensor attack and deluge attack are the three main application layer DoS attacks in WSN.

1) PATH-BASED ATTACK

A path-based DoS (PDoS) attack can deplete the battery power of several nodes in WSNs. A standard tree structure topology of WSN has the potential of disabling a wider area when compared to a simple path [52]. A typical PDoS attack is initiated by first compromising member nodes before flooding intermediate and sink nodes with spurious and replayed packets along the routing paths. This attack consumes resources along the path of the base station, thereby denying legitimate nodes access to the resources.

2) OVERWHELMING SENSOR ATTACK

In this type of attack, the attacker stimulates sensor nodes by continually triggering communication [42]. This, thereafter causes the network to forward large volume of traffic towards the base station to consume the node's bandwidth and energy recourses.

3) DELUGE ATTACK

WSN protocols, such as TinyOS's Deluge network programming system, has the capacity to allow remote reconfiguration of nodes deployed in remote environments. Most of these systems are often used in a trustworthy environment, therefore if the reconfiguration process is not secured, an attacker can take advantage of this and hijack the process [42]. Large portion of the WSN can be short down by a Deluge attack to deny legitimate users resources and services.

Table 1 gives a comparative summary of different forms of DoS attacks targeting sensor components, at different layers

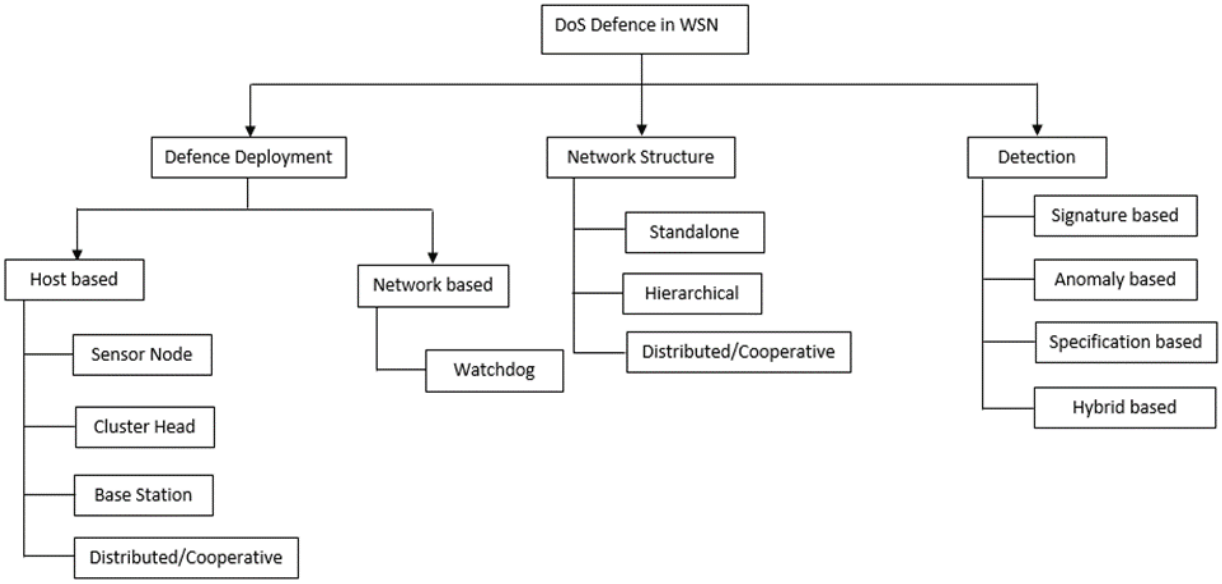

FIGURE 4. DoS defence taxonomy in WSN.

of the WSN, as obtained in the reviewed literature. It is observed that there are more reported and discussed cases of DoS attacks in the last three layers (i.e. network, link and physical) as compared to the first two layers (i.e. application and transport).

V. WSN DoS DEFENCES

Several DoS defence solutions have been proposed in WSNs; which are often lightweight, due to the resource constraints of the sensor nodes. Depending on the architecture, WSN is composed of several sensor nodes and a base station. As mentioned earlier, hierarchical WSN is organised into clusters with cluster heads. The cluster heads perform additional tasks when compared to the ordinary cluster members, therefore, the latter has a better battery life, software capability and hardware capability. In this section, we will focus on DoS defence proposed for WSN by categorizing them according to the technique used, defence network structure and their deployment location by presenting a taxonomy (see Fig. 4.).

A. WSN DoS DEFENCE DEPLOYMENT

DoS defence for WSNs can be deployed in two main locations, host-based and network-based. Host based defence deployment can be further classified into sensor node deployment, cluster head deployment, base station deployment and distributed/collaborative deployment; while network-based defence deployment are made up of watch dog sensor nodes.

1) HOST-BASED DEFENCE DEPLOYMENT

Host-based deployments in WSNs are defence techniques deployed on the sensor nodes to detect the presence of DoS attack. In host-based deployment, the intrusion detection system (IDS) can be deployed on the ordinary sensor nodes, cluster heads and base station. A cooperative/distributed deployment can also be achieved, where the IDS deployed interact to determine the presence of an attack. An attack in WSN can be directed towards the ordinary sensor node, therefore, we consider the sensor node as a standalone device (host-based defence).

a: SENSOR NODE DEPLOYMENT

The sensor nodes are the smallest unit in the WSNs which are deployed to monitor and capture information of interest from the environment. The information collected are thereafter sent to the cluster head, in a cluster-based structure. DoS defences deployed on the sensor nodes are usually lightweight and used to monitor traffic patterns and resource usage to detect an anomaly. Salmon *et al.* [53] propose a host-based IDS defence deployment. The IDS is deployed on all the sensor nodes using danger theory immune-inspired technique to detect the denial of sleep attack. Boubiche and Bilami [54] studied energy depletion attacks in WSN and proposed an energy efficient cross layer security mechanism to mitigate denial of sleep attack. Each of the sensor nodes use the information on the MAC layer to determine the source of the packet to be received. Thereafter, received signal strength indicator value and the routing information are used to check the identity of the attacking node.

b: CLUSTER HEAD DEPLOYMENT

In a cluster-based topology, the cluster heads aggregates data from the sensor nodes in its area and forwards it to the base station. The cluster heads are usually of higher capacity than the ordinary nodes (i.e. higher energy, memory, computing and power), therefore many proposed DoS defence solutions have been deployed in the cluster head. Furthermore, its

centralized placement between the sensor nodes and the base station gives the deployed defence more control over the connected nodes. Yan *et al.* [55] propose a hybrid-based IDS in a cluster-based WSN using anomaly detection module and misuse detection module. The former is used to filter the abnormal packets from the normal packets while the latter is used to detect the type of attack. The result of the two-detection module is used as an input to the decision making module to determine the presence of an intrusion and the class of attack. The proposed IDS was deployed in the cluster head to screen packet to detect attacks, such as DoS. A hierarchical based intrusion detection system was proposed by Mamum and Kabir [56] using a hierarchical overlay design. Just like the case of [55], the IDS in [56] combined signature-based and anomaly-based techniques to detect both known and novel attacks. Core defence strategy was used by deploying the IDS on the cluster head, which is the centre point, to optimize the energy consumed.

c: BASE STATION DEPLOYMENT

In WSN, sensed and measured data from the cluster heads are forwarded to the base station through multi-hop routing. The base station is saddled with the responsibility of monitoring all cluster heads within its coverage area. Dallas *et al.* [57] propose a hop-count monitoring scheme to detect sink hole attacks in WSN. This approach detects abnormal route advertisement by monitoring the advertised hop-count values. A significant change in the hop-count value is an indication of sinkhole attack. Given the resource constraints of sensor nodes, the intrusion method was deployed in the base station to monitor the consistency of the traffic arriving. To detect selective forwarding, a DoS attack in WSNs, Kaplantzis *et al.* [58] proposed a centralized IDS deployment by performing all the intrusion detection tasks (i.e. feature selection, data processing and anomaly detection) in the base station. The IDS adapts a simple classification approach based on support vector machines (SVM) and sliding windows to detect the DoS attack, by using routing information local to the base station.

d: DISTRIBUTED/COOPERATIVE DEPLOYMENT

A cooperative defence deployment involves the distribution of defence solution on all the sensor nodes in the WSN, to detect DoS attacks at all levels. A sensor node that detects an anomaly with strong evidence can solely determine that the network is under attack and can initiate a counter response. However, when a node detects an anomaly with a weak or inconclusive evidence, a cooperative mechanism can be initiated with neighbouring nodes to form a global defence action [59]. Notwithstanding the certainty of the detected anomaly by the sensor node, a cooperative decision guides against false alarm. A distributed pattern recognition method for detecting node exhaustion attacks, such as DDoS, in WSNs was proposed in [60]. This attack detection scheme consists of five phases of operation (i.e. initialization, observation, communication, verdict and pattern update), to be carried out sequentially, to guarantee the availability of sensor nodes. During the decision-making process, a single traffic observation cannot produce a conclusive decision about an attack, therefore, sub pattern values are employed to facilitate the decision-making process. Shamshirband *et al.* [61] propose a cooperative fuzzy artificial immune system (Co-FAIS) to detect DDoS attack in WSNs. Co-FAIS is a modular-based defence strategy, acquired from the danger theory of human immune system, that integrates the cooperative artificial immune system with fuzzy Q-learning algorithm. It functions by ensuring cooperation between detector sink node agents (i.e. cluster heads) and response base station, to defend against potential DDoS attacks that affects the availability of resources in WSN.

2) NETWORK BASED DEFENCE DEPLOYMENT

Network based defence deployment monitor the network traffic of a specific area and subsequently analyse its activities to detect an anomaly. In WSN, network based defence are passive or active techniques that listens to the network transmission, retrieve and examine the transmitted packets to detect an anomaly. They have an advantage of being able to monitor large number of hosts to detect attacks originating or directed towards multiple hosts with minimal deployment cost. One of the major drawbacks of the network based defence deployment is its inability to detect local and encrypted attacks [62]. An example such deployment is the watchdog.

Watchdog: The watchdog mechanism is used to monitor and identify anomalies in WSN by promiscuously listening to the next-hop node in the packets path. It propagates the evaluated results to other nodes by broadcasting. Watchdog is the base of common misbehaviour detection techniques and trust or reputation system [50]. It maintains a buffer of recently sent packets and compares each overheard packet with the packet in the buffer to find a match [50]. If there is a match, the watchdog discards the packets in the buffer since it has been forwarded. If the monitored node drops packets above the accepted threshold set and there is no match, the source node of the communicating party is notified. An extended watchdog was proposed in [63] to increase the watchdog's monitoring neighbours beyond one-hop. It ensures that the watchdog node is aware of its neighbour's behaviour when the MAC control packets are enabled. Furthermore, a technique that optimally monitor neighbours, spontaneous watchdog, has been proposed by Roman *et al.* [64]. The spontaneous watchdog harnesses the broadcast nature of communication networks to benefit from the high density of sensor nodes deployed in the target environment. For every packet transmitted in the network, there are nodes that are available to receive both the packet and the relayed packet by the next-hop. Therefore, all nodes have the ability to activate their global agents to monitor those packets.

Table 2 presents a comparative summary of the evaluation of different defence deployment in WSN.

TABLE 2. Evaluation of DoS defence deployment.

Defence deployment	Detection speed			Efficiency			Overhead		
	High	Medium	Low	High	Medium	Low	High	Medium	Low
Sensor node	✓				✓		✓		
Cluster head		✓			✓			✓	
Base station		✓			✓			✓	
Cooperative			✓	✓			✓		
Watch dog	✓				✓				✓

B. WSN DoS DEFENCE NETWORK STRUCTURE

The network structure of DoS defence in WSN can be categorized into three, namely: standalone defence, distributed/cooperative defence and hierarchical defence [65] [56].

a: STANDALONE

In a standalone defence, each sensor node is equipped with a defence agent that is autonomous of the defences on other nodes [65]. The defence agent runs independently without exchanging information with other nodes, therefore it is responsible for detecting attacks by itself. The functions of standalone deployment are limited; therefore, it can only be suited to environments where the sensor nodes have the capacity of running a defence agent.

b: DISTRIBUTED/COOPERATIVE

As in the case of distributed/cooperative deployment, a cooperative network structure involves the collaboration of defence agents in the sensor nodes to form a global defence system. This network structure is suitable for flat WSNs where a global defence is triggered, in the event of an inconclusive detection by individual nodes [56].

c: HIERARCHICAL

This is an extended version of distributed/cooperative network structure, where all sensor nodes are equipped with defence agents and detect attacks locally. The hierarchical network structure is made up of cluster heads and member nodes, therefore, the cluster heads will be responsible for monitoring its own member node packet [65]. The network is alerted when an attack is detected.

C. DoS DETECTION IN WSNs

Typical DoS detection techniques in WSN can be functionally categorized into four, namely: misuse or signature based, anomaly based, specification based and hybrid based; to classify data traffic as either legitimate or malicious. These techniques are built on the assumption that there exist a seemingly observable difference between the conduct of an attacker and that of a legitimate node [8]. Therefore, the deployed detection techniques can match the preprogramed or learnt rules.

1) SIGNATURE BASED DETECTION

Signature based detection technique profiles previously known attack patterns, as a reference, before storing in a knowledge database to detect future attacks. An attack signature can either be a univariate or multivariate data sequence, where traffic patterns are monitored and captured in the network and compared with existing signatures to detect attacks. Signature based detection is also referred to as misuse or rule based [9] due to the knowledge accumulated about specific attacks over time [66]. The common anti-virus solution is a typical example of a signature based solution.

A rule based intrusion detection that can detect DoS attacks in WSN was proposed by Yu and Tsai [67]. They used a machine learning algorithm, SLIPPER, to build a detection model that consists of multiple binary classifiers with certain set of rules. Each rule learnt from the dataset during the training phase might not have a very high prediction accuracy on new data, however, the predictions based on the entire set of rules are expected to be largely true and effective. During attack detection, the detection agent will analyse both the packet data and the local data from suspicious nodes to detect an attack. Da Silver *et al.* [68] propose a decentralized IDSs installed on common sensor nodes and distributed around the network to detect attacks. This technique is divided into three phases; the data acquisition phase, the rule application phase and the intrusion detection phase. During data acquisition, the nodes are set to a promiscuous mode to collect data; thereafter, important information are extracted before storing

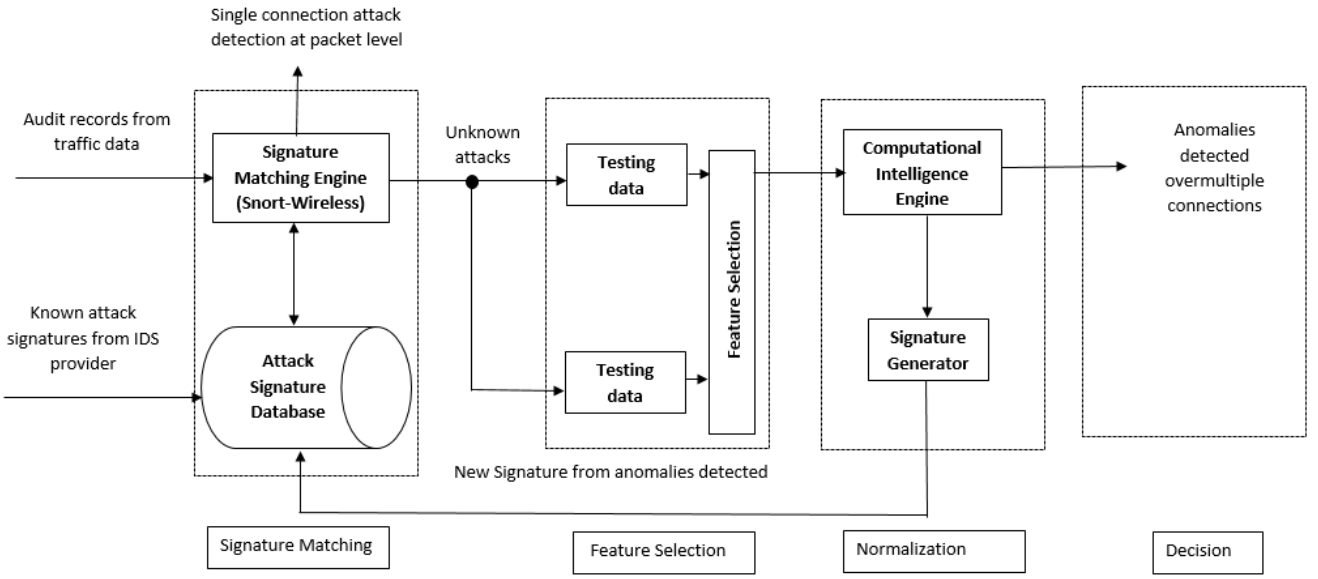

FIGURE 5. Intelligent intrusion detection and prevention system (IIDPS) architecture for WSNs (adapted from [69]).

for subsequent analysis. The rule application is the processing phase where pre-set rules are applied to the stored data to determine a failure. Lastly, the intrusion detection analyses the ratio of the amount of failures to the expected amount of occasional failures, in the network, to detect an attack.

Shamshirband *et al.* [69] in their work discussed a model of intelligent intrusion detection and prevention system (IIDPS) to detect attacks in WSN. Its architecture is made up of four modules, namely: signature matching, feature selection, normalization and decision (see Fig. 5). The signature matching engine of the IIDPS model audits the network traffic records using the Snort-Wireless to ensure that all known attacks are detected at packet level. For unknown attacks, the signature matching engine sends an alarm to the feature selection module, when it cannot detect correct attacks. The feature selection module detects unknown attacks by training and testing algorithms to build a corresponding model. The feature selection stage is introduced to remove some noise or redundant features to reduce the data dimension. Thereafter, the data are normalized through the normalization module and subsequently used to train the computational intelligence engine to form a model. A signature matching module is generated by the normalization module for inspection. Finally, the decision module is used to evaluate the generated model, through the computational intelligence engine, and compared against the monitored traffic. If this scheme detects a deviation that either exceed or fall below (in case of abnormality model) a predetermined alarm threshold, the detection stage will be activated.

Anjum *et al.* [70] propose an intrusion detection module based on the principle of minimum cut set and minimum dominating set, for a distributed deployment, using a signature based detection technique. The IDS deployed on various nodes monitor the network, in order to detect the presence of malicious packets, during transmission between the adversary and the destination node. Two types of sensor nodes were considered, the tamper resistant sensor (TRS) and the non-tamper resistant sensor (non-TRS). An assumption was made that an adversary can compromise one or more non-TRS while the TRS cannot be compromised. The minimum dominating set was used to divide the network into clusters, while the cluster heads are used with the destination to determine a minimum cut set. The detection modules are, therefore, placed on all the nodes in the minimum cut set. Simulation results from their work shows that the effectiveness of a signature based intrusion detection technique is majorly dependent on the placement of the detection modules.

Cho *et al.* [71] propose a partially distributed IDS, with low power and memory demand, to detect DoS attack in WSNs. Bloom filters was deployed to reduce the code size of the attack signature, by using a classification method that spreads these signatures among multiple Bloom filter arrays. When malicious packets transverse the relay nodes where IDS is installed, the relay nodes detect the attack using the signature in the IDS. Supposing the packet is fragmented, the attack signature will be divided into several packets to detect the attack. The attack can also be detected at the application layer when the fragmented packets are reassembled. Results obtained from this work show that the proposed method eliminates data overhead, which accounts for a significant amount of the energy consumed.

A centralized IDS approach that detects blackhole and selective forwarding attacks in a cluster-based WSN has been proposed [72]. The IDS uses well-known attack signatures to detect attacks by deploying it in the base station to save energy. The IDS is executed periodically during each

communication round and segmented into three phases, namely: data collection, rule control and intrusion detection phase. In the data collection phase, all the sensor nodes that are cluster heads must send a control packet to the base station. Thereafter, in the rule control phase, signature rules are applied to all the received data. Lastly, in the intrusion detection phase, the base station detects and identifies the attacker by relying on the previous phase. An alarm is sent to all sensor nodes in the network to block future communications with the attacker to avert further damage.

Signature based detection in the context of WSN is a non-trivial task. Practically, it is difficult to reason as attackers do, therefore the network administrator must have to model attack patterns according to attacks that can arise in future [8]. Furthermore, the resource constraints of WSNs makes the implementation of the signature based detection difficult, due to the need to store more attack signatures. Typically, signature based detection technique is known for its accuracy when detecting known attack signatures, provided the database is up-to-date. The major drawback of signature based technique is its inability to detect unknown attacks and variation of known attack signatures, which can lead to high false negatives.

2) ANOMALY BASED DETECTION

Anomaly based detection technique for DoS attacks in WSNs involves the profiling of normal traffic behavioural pattern, over a pre-determine period, with the aim of detecting subsequent patterns that deviates from the profiled or expected behaviour [6]. Profiles are developed from many attributes and can be either dynamic or static. Anomaly based detection is also referred to as behavioural based detection in some instances. During attack detection, anomalies can be categorized into three, namely: point anomalies, contextual anomalies and collective anomalies [73].

Point anomaly is the simplest type of anomaly that occur when an individual data instance is deemed anomalous with respect to the rest of the data [73]. When an anomaly is contextual, the data is anomalous in a particular context but not in another context. This is majorly determined by the format of the dataset. Anomaly is referred to as collective when a group of data instances are anomalous with respect to the entire dataset. A practical example of this is the DDoS flooding attacks, where an individual data instance can only become anomalous and harmful in coordination.

Anomaly based detection involves two phases, namely: training and detection phase. In the training phase, the accuracy of anomaly detection is based on the type of input data. Input data is a collection of instances such as samples, patterns and observations, described by set of attributes in form of binary, numerical or categorical. Each of the data instance may consist of single attribute (univariate) or multiple attributes (multivariate). Multivariate data instance can either be the same type or combination of different data types [73]. Labels in dataset are used to tag a particular instance as either normal or anomalous. Almomani *et al.* [1] constructed a specialized WSN dataset, WSN-DS, using LEACH protocol. WSN-DS contains 374,661 records representing four different types of DoS attacks, namely: grayhole, blackhole, scheduling and flooding. Additionally, it also contains normal instances when no attack exists. In the detection phase, anomaly detection exists in three modes, depending of the available labels, namely: supervised, semi-supervised and unsupervised.

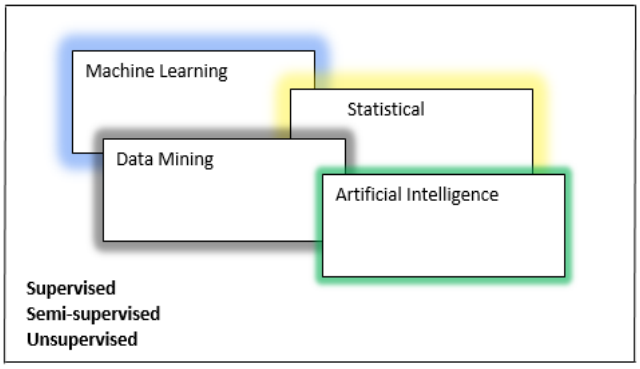

FIGURE 6. Anomaly detection technique is WSNs.

In supervised approach, it is assumed that there are labelled instances of training dataset for both normal and anomaly classes. This approach is often used to construct predictive models for normal versus anomaly classes, where previously unseen data instances are matched against the model, to determine the class it falls into. Two major issues of supervised anomaly detection have been identified by Bhuyan *et al.* [74]. Firstly, in training data, anomalous instances are fewer when compared to normal instances; secondly, lack of accurate and representative label can lead to a classification challenge for anomaly class. In semi-supervised anomaly detection, it is assumed that the training data only contains label instances for normal class. Semi-supervised anomaly detection presents a much more practical approach as compared to supervised technique, as they do not require labels for anomaly class [73]. Lastly, in the unsupervised anomaly detection approach, training dataset is not required, which makes it one of the most widely deployed techniques [74]. It assumes that the normal data instances highly surpass the anomalies, in a typical test dataset. However, if this assumption is not true, the technique will suffer from high false alarm rate.

The reporting of detected anomalies is a very crucial aspect of anomaly detection. From the literature, the two common detection output types are labels and scores. Labels involve assigning an indicator to each test instance, signifying either normal or anomaly. Scores, on the other hand, involve the assigning of anomaly score to each instance data to show the degree of anomaly.

Existing anomaly techniques to detect DoS attacks can be grouped into four classes, namely: statistical, machine learning, data mining and artificial intelligence (see Fig. 6).

a: STATISTICAL ANOMALY DETECTION

In statistical anomaly detection, statistical features of normal traffic pattern (without any attack) are collected and profiled to produce a normal traffic pattern. This profile is based on network metrics such as packet inter-arrival rate, number of different IP addresses, number of packets for each protocol and connection rate [75]. During the monitoring stage, the referenced normal traffic profile is compared with packets in the network, during transmission, to generate an anomaly score. If the score is higher than a predetermined threshold, the detection system will flag the presence of an anomaly. During attack detection, statistical distribution (e.g. Poisson), statistical measure (e.g. mean, variance etc.), statistical model (e.g. auto regression) and statistical inference test (such as parametric and nonparametric), are used to determine the legitimacy of traffic behaviour.

Ho *et al.* [76] propose a statistical decision process, Sequential Probability Ratio Test (SPRT), to detect mobile malicious node attacks, such as DoS, in static WSNs. This technique provides a distributed detection approach, by applying sequential hypothesis test to identify nodes that are unusually silent over a long period of time. They leverage on the fact that static nodes are always around their neighbours and communicate frequently with them. Malicious mobile nodes, on the other hand, are always revolving, therefore, they are silent in their previous location before moving. SPRT is a dynamic threshold scheme, where a random walk moves between a dynamically configured upper and lower limits according to its observation. If the observation exceeds the upper limit or falls below the lower limit, it terminates the acceptance of the alternative hypothesis. Simulation results show that the proposed technique can detect malicious mobile nodes using very few samples, with a low false positive and false negative rate.

Sun *et al.* [77] propose an extended Kalman filter (EKF) based method with the combination of cumulative summation (CUSUM) and generalized likelihood ratio (GLR), herein called CUSUM GLR, for anomaly detection in WSNs. The EKF monitors the behaviour of neighbouring nodes to predict their future states. By using a threshold-based mechanism, it can promiscuously listen to transmitted aggregated values and compare it with a locally computed normal range, to determine if there is a significant difference. CUSUM GLR is introduced to increase the detection sensitivity when there is a little deviation in the malicious values. Experimental results of EKF and CUSUM GLR on a representative sensor node, MICA2 mots and large-scale synthetic data, show that the proposed method is practical on resource constrained nodes and can detect intrusion.

Fragkiadakis *et al.* [78] propose a combination of simple threshold algorithm and CUSUM change point detection, by monitoring the received packets to uncover changes in the statistical features of the signal-to-noise ratio (SNR), to detect the physical layer jamming attacks in WSN. Among the SNR-based metrics considered in a short window are minimum SNR, average SNR and max-minus-min SNR. Using a modified version of the madwifi driver, SNR was the preferred metric as against other metrics such as the number of PHY errors, because wireless device drivers and hardware radio interfaces provide SNR values for the received packets. The proposed algorithm was applied on the measurement obtained from two locations, far and close to the jammer. The results obtained show that the CUSUM detection method improves the detection probability and false alarm rate for cases where measurements were taken far away from the jammer. This proposed technique can also improve the robustness of the system, using different detection threshold values. Similarly, Huang *et al.* [79] propose Markovian IDS to protect sensor nodes from malicious attacks. Markovian IDS incorporate game theory to achieve the integration of IDS within WSNs. Furthermore, Markov Decision Process (MDP) is used to improve the self-learning process of the IDS, to detect sensor node attacks. The MDP can predict future points of attack to device suitable defence strategy.

In WSNs, sensor nodes can be compromised to launch a DoS attack to deplete the energy and resources of legitimate nodes. To mitigate against this, Ballarini *et al.* [80] propose a dedicated inspector control node, herein called cNodes, to analyse network traffic inside a cluster, in a hierarchical cluster WSN. The cNodes does not perform sensing or monitoring, but only function to detect DoS attacks and send warning signals to the cluster head, when an anomaly is detected. Markov chain models and formal models, in form of generalized stochastic Petri nets (GSPN), were used to represent DoS detection mechanisms with relevant steady-state measure. Simulation results obtained, using a network simulator, NS-2, show that the cNodes dynamic allocation can guarantee a uniform energy consumption with an efficient attack detection capability.

Boa *et al.* [81] propose a trust-based IDS to detect anomaly in WSN. To describe the behaviour of sensor nodes and cluster heads during intrusion detection and trust evaluation, the authors developed a probability model based on stochastic Petri nets technique. Statistical method is used to predict the probability of false alarm of the trust-based IDS method. Simulation results show that the compromised nodes can be easily detected, with the detection accuracy of trust-based IDS indicated. Similarly, a simple statistical model of neighbours behaviour and a low complexity detection algorithm has been proposed by Onat and Miri [82]. This model monitors the received packet arrival rate and power level, using a packet count based sliding window approach, to detect an attack. The last N packets received from each neighbour node are used to calculate the statistics of that neighbour, and each packet that arrives is compared with these values. If packet correlates to the statistics of the neighbour, it is classified as a normal packet and used for subsequent new calculations.

To detect a distributed segment-based anomaly, such as DoS and sinkhole attacks in WSNs, Xie at al. [83] proposed a combination of Kullback-Leibler (KL) divergence approach and kernel density estimation (KDE). This method aims to detect long term anomalies to meet the resource constraints

of WSNs. The probability destiny function (PDF), tracked by the distributed segment-based recursive KDE, is used to make decisions through the analysis of variations taking place in the sequence of the KL divergence between every two temporally successive PDF. Using an approximated KL divergence ensures that the cost of communication is highly reduced. A numerical experiment conducted, using the real-world received signal strength dataset from Mica2 network deployment at the University of Michigan, shows that the proposed technique is efficient and effective.

The devastating effect of blackhole attacks that consume resources in WSNs, to the detriment of legitimate nodes, has necessitated the proposal of an unmanned aerial vehicles (UAVs) using a sequential probability ratio test (SPRT) [84]. SPRT is a statistical sequential hypothesis test used for decision making process. It can be applied to test process to generate rules to either accept the hypothesis when a certain threshold is attained, or to continue the experiment to observe new values. This method uses SPRT as a dynamic threshold to detect and block malicious nodes in the network. Simulation results using mobile agents to detect blackhole attacks in NS-2 show a decrease in computation time and an increase in reliability and scalability. Assad *et al.* [85] propose the adoption of probabilistic intrusion detection models, named single/multi-sensing detection, to detect intrusion in WSNs. The probabilistic model is used to derive an analytical expression to characterize the topological features of a network coverage. This is used to design and analyse the probability of intrusion detection in homogeneous WSN. Various parameters such as node density, sensing range, node availability and intrusion distance are considered to enhance the quality of the node deployment to detect an attack.

Shafiei *et al.* [86] propose both centralized and distributed monitoring approach to detect and mitigate sinkhole attacks using geostatistical hazard model in WSN. The idea behind the proposed technique is that nodes around the sinkhole deplete their energy faster than other nodes in the network, since most sinkhole nodes advertise a shorter route to the base station, thus they are frequently used. Therefore, an energy hole is form around each sinkhole. The base station uses a geostatistical approach, by sampling the residual energy in each sensing region, to estimate the possibility of the occurrence of a sinkhole attack, using an extracted statistical estimator. Depending on the value of the estimator, the base station may inform all the nodes to refrain from suspicious regions in their routing. The distributed monitoring approach detects regions with a lower average residual energy level. Simulation results during the evaluation of the proposed method, using Castalia simulator based on OMNeT++, show that the proposed method successfully prevent nodes from transmitting data traffic towards the reported suspected regions. This, therefore, changes the energy expended around the sinkholes and the energy pattern of the network remain intact.

Ye *et al.* [87] propose a statistical approach based on extracted covariance features from a temporal sensor data to identify attacks in WSNs. The mapping in the covariance feature space is used to group the original observations into time sequence before converting to covariance feature space. Anomalies in the network are detected using the Mahalanobis distance. Ghosal and Halder [88] in their work identified the vulnerability of uniform random deployment in WSNs and proposed a tailor-made Gaussian distribution strategy to protect the network. Intrusion detection problem was investigated by considering both single and multiple sensing detection scenario under a realistic probabilistic sensing model. The results obtained show that the proposed approach performs better than the other related methods.

Statistical techniques allow the learning of expected normal behaviours by observing, to enhance the detection process. An anomaly score associated with statistical methods can further be used as a confidence interval during the decision-making process. Demerits of statistical anomaly can be attributed to the challenges faced to achieve an optimal threshold setting. Additionally, statistical anomaly detection may also involve making some hypotheses and assumptions. If this is not fundamentally justified, it can lead to high misclassification rate.

b: MACHINE LEARNING ANOMALY DETECTION

Machine learning anomaly detection techniques involve the establishment of an implicit or explicit model to ensure patterns are analysed to be categorised [75]. One of its key attribute is the need for a labelled dataset to train the behavioural model, which places high demand on the limited resources of sensor nodes in WSNs. In many cases, deploying machine learning encapsulate other techniques, such as data mining and statistical methods, however, it is slightly different from statistical methods. Statistical methods require an understanding of the process that produces the data; while machine learning has the capability of building a system to improve the detection performance based on the previously obtained results [6].

Kaplantzis *et al.* [58] propose a centralised intrusion detection method based on Support Vector Machine (SVM) to detect selective forwarding DoS attacks in WSNs. SVM is a machine learning algorithm which was originally intended for binary classification but has been expanded to include density estimation, regression and one-class classification among many others. This approach is based on one-class SVM and uses the local routing information (bandwidth and hop count) of the base station to detect an attack. The choice of the base station is to provide a centralised approach to conserve energy resources of the sensor nodes. Network simulations was carried out in OMNET++ and all the SVM training and testing used a modified version of SVMheavy. Results presented show that the proposed method can detect blackhole attacks with an accuracy rate of 100% and selective forwarding attacks with 85% accuracy. A Linear Programming-based Fuzzy Constraint (LP-FC) and foresight response strategy based on Support Vector Data Description (SVDD), herein called LP-FCSVDD, has been proposed by

Ghasemigol *et al*. [89] to detect anomalies in WSNs. Just as in [58], SVDD is a one-class classification method that presents a lightweight foresight response technique to resist all forms of anomaly. The LP-FCSVDD is used to solve the decision boundary issue when noisy data samples exist in the training set.

Furthermore, a one-class SVM centred hyper spherical and hyper ellipsoidal for anomaly detection in WSNs has been proposed by Rajasegarar *et al.* [90]. This technique consists of two approaches, linear programme-based hyper ellipsoidal formulation, which is referred to as centred hyper ellipsoidal support vector machine (CESVM) and a distributed anomaly detection algorithm using a one-class quarter-sphere support vector machine (QSSVM). The hyper sphere function by collecting normal packets vector in a higher dimensional space for each sensor node. The global hyper sphere collects all the summary information about the hyper spheres communicated among the nodes. The sensor nodes, thereafter, use this to detect anomaly in the network. Simulation result shows that CESVN and QSSVM formulations can achieve a high detection rate on different real and synthetic datasets.

A cooperative game theory approach, using fuzzy Q-learning technique for detecting DDoS attacks in WSNs has been proposed by Shamshirband *et al.* [91]. The cooperative game-based Fuzzy Q-learning (G-FQL) is a strategy game consisting of three players, the base station, sink nodes and the attacker. The strategy based cooperative game uses a continuous learning of past behaviours in the fuzzy Q-learning (FQL) decision making process to detect attacks. The game only starts when the victim node senses a flooding attack that overwhelms it, above a predetermine alarm threshold. To determine the different adversaries that can be encountered by the node, FQL is used to reinforce the players self-learning abilities. It gives detector players an incentive function to protect the vulnerable nodes that can be a potential security threat.

Misra *et al.* [92] propose a learning automation based IDS (LAID) for intrusion detection in WSN. The LA-based approach is centred around automation, environment and action probability updating scheme; and uses the packet sampling concept by juxtaposing it within the settings of the LA. The proportion of the sampled packets detected to be malicious is used to determine the feedback of the environment.

Pattern recognition, a branch of machine learning approach, has been proposed by Braig [60]. The distributed pattern recognition approach observes the normal network traffic flow to differentiate between legitimate and anomaly traffic packets. The detection process consists of five stages, namely: initialization, observation, communication, verdict and pattern update. All other stages apart from the initialization stage needs to be executed within a certain time interval of fix duration. Attack detector nodes in the network are referred to as GN nodes, while a subset of GN nodes that are selected as decision making nodes are referred to as mGN node. During the initialization stage, node identification tags and topologies are established. Thereafter, the GN and mGN are selected by the base station to operate as part of the attack detection process. The observation phase ensures each GN node monitors the packet initiation or transmission that transverse through regions of operation, destined for the target nodes. In the communication phase, GN nodes communicate directly with two other adjacent nodes (i.e. successor and predecessor) to form a GN array. During the fourth phase, the verdict phase, each mGN expects half of the GN nodes, within their local region, to send them a Boolean-valued signal for each of the targets in order to confirm an attack. Finally, the pattern update phase is used to constantly store update of pattern values in the pattern tables of the GN nodes. The frequency of the update will determine the accuracy of the pattern recognition method.

Li *et al.* [27] proposed an IDS based on K-nearest neighbour (KNN) to detect DoS flooding attacks in WSNs. Firstly, the proposed system separates normal nodes from abnormal before analysing the parameter selection and error rate of the IDS. In the application of KNN, the approximate value of K is a key factor that affect its cost and effectiveness, while the detection error rate is directly affected by the cut off value. The KNN detection algorithm uses the abnormal feature of an adversary node that sends frequent RREQ messages than normal nodes in a flooding attack. Comparing the frequency of the sent RREQ messages by nodes in the network, the adversary nodes can be detected. Experimental results using GAINZ Zigbee nodes and TinyOS operating system show an improvement in the wireless ad hoc on-demand distance vector routing protocol (AODV) which achieves a fast and efficient intrusion detection.

He *et al.* [93] propose a multitask learning-based forecast method to detect security attacks in WSNs. This method partitions the topology of a large-scale WSN and determines the level of similarity among the regional subnetworks. The multitask learning can use the occurrence and transmission features of known network security event to predict the trend of the unknown network security events. The quantitative trend of unknown regional network security event can be determined if there is no regional data. This work used a forecast method, Prediction Network Security Incomplete Unmarked Data (PNSUID), to predict missing attack data in the target region. Results from the work show that PNSUID method, when compared with the traditional SVM, is more effective in detecting attacks.

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. Overheads can also cause bottleneck in the network, which can subsequently lead to the degradation in performance of the sensor node. Overall, machine learning anomaly detection methods have a relatively high efficiency in detecting DoS attacks in WSNs and can change their execution strategy based on any extra acquired information.

c: DATA MINING ANOMALY DETECTION

The significant increase in the amount of data to be processed in WSNs complicates the effort to detect DoS anomaly pattern. Data mining anomaly detection approach, therefore, provides an information extraction method to discover hidden facts in the databases. It functions by scanning through the data to determine patterns and establish a relationship between them. Data mining include different parameters such as sequence analysis, association, clustering, classification and forecasting. Sequence analysis involves identifying patterns in an event to deduce subsequent events while association looks for a common attribute that connects one event to the other. Clustering finds previously unknown visually documented groups of fact while classification search for new patterns. Lastly, forecasting uses the discovered data patterns to reasonably predict the future. A typical data mining process involves a data pre-processing stage that often a times use up 80% time of a data mining effort.

Garofalo *et al.* [94] propose an IDS using decision tree to detect sinkhole DoS attacks in WSNs. The proposed IDS is made up of a Central Agent (CA) and numerous Local Agents (LAs), with each LA deployed on sensor node and the CA installed on the server that function as the base station for the WSN. The LA is made up of local packet monitor, control data collector and local detection engine. The local packet monitor is used to monitor the traffic that is transmitted through the nodes where the LA is deployed. Control data collector measure parameters within the network for upward transmission to the CA, while the local detection engine carry out detection activities locally, receives response messages from the CA, raises alert when attack it detected and recover events if need be. The decision tree uses a supervised dataset for training by splitting it into homogeneous subsets. During the intrusion detection process, the decision tree search for the features that best describe the condition under a given attack and when there is no attack, using the available representative dataset. Experimental results obtained from the simulation of sinkhole attack on AODV routing protocol in NS-3 using decision tree show that the proposed method, when compared with other related methods, has a high detection rate and low false positive.

Moshtaghi *et al.* [95] propose a distributed anomaly detection technique using a clustering ellipsoids in non-homogeneous WSN environment. In this technique, each sensor node reports a hyperellipsoid that characterize the locally observed distributed measurements at each sensor node. The central base station, thereafter, receives these hyperellipsoids and cluster the local hyperellipsoid, to ensure that the resulting clusters characterize the underlying modes of the distribution of the measurement in the network holistically. The set of hyperellipsoid cluster in the network can be used as the basis of anomaly detection by each of the sensor nodes. Results from the work, using a real-life dataset (Intel Berkeley Research Laboratory dataset) and a synthetic dataset, show an improved accuracy and a lower complexity than the centralized methods based on clustering raw data. Similarly, another clustering algorithm, density-based fuzzy imperative clustering algorithm, herein referred to as D-FICCA, has been proposed by Shamshirband *et al.* [96] to detect DDoS in WSNs. The proposed system combines fuzzy sets element with density-based spatial clustering of applications with noise (DBSCAN) to ensure D-FICCA adapts to the base station agent to enhance the detection of an incoming distributed form of DoS, DDoS, that floods the WSN to cause congestion and downtime. D-FICCA is used to identify the data distribution of an anomaly profile that affects the behaviour of a sensor node. The imperialist competitive algorithm (ICA) is developed as a result of the continuous self-learning from previous attack models and the behaviour in the fuzzy learning decision making process, for attack defence.

Mansouri *et al.* [97] propose a clustering technique in WSN to detect DoS attacks. This technique is based on hierarchical clustering, where sensor nodes in the network elect control nodes (Cnode) that analyse the traffic within a cluster and sends a warning signal to the cluster head, whenever an anomaly is detected from compromised nodes. These compromised nodes have the ability to generate malicious packets to flood the entire network. The proposed technique is dynamic as ordinary sensor nodes in each cluster periodically elect Cnodes to ensure an energy balance and good coverage within the network.

A data mining approach that combines both clustering algorithm and classification algorithm has been proposed by Kaur and Singh [98] to detect blackhole attacks in WSNs. K-means and J-48 clustering algorithms were deployed due to their efficiency. The experimental work involves two stages; the creation of WSN using NS-2 and the extraction of dataset to perform data mining task. The behaviour of all the nodes in the network is monitored to determine if it is receiving the number of packets sent from the source node. Nodes that drops a fraction of packets been transmitted along its path are regarded as blackhole nodes. A combination of two IDS algorithms have been proposed in [99]. The first IDS uses a supervised learning approach and is deployed on the level of the sensor nodes while the second use an unsupervised learning approach and is deployed in the level of the sink node and base station. The supervised learning, on the level of the sensor node layer, is implemented to detect intrusion by selecting a candidate pair (feature, value). The unsupervised learning used on the level of the sink and base station is based on a decision tree, J48, and is used to handle the learning scheme in the sensor node layer.

Fouchal *et al.* [100] propose a recursive clustering-based method to detect DoS attacks in WSN. This approach recursively clusters the network until the desired granularity is achieved using Fast and Flexible Unsupervised Clustering Algorithm (FFUCA), which is based on ultra-metric properties and LEACH algorithm. The FFUCA is used to optimally deploy sensor nodes to preserve energy and detect attacks.

In general, data mining anomaly detection techniques are able to address the limitations of other techniques (non-data mining) by dealing with large datasets. Important features

are extracted to transform the dataset into a logical structure to achieve an improved DoS attack detection. Deploying data mining also enhance the security expert to differentiate between normal and attack traffic using bounds. However, data mining techniques presents some few drawbacks, for example if there are missing or bad values from the dataset, the efficiency of the detection will be affected. Also, attribute selection of large datasets can present its own issues which may worsen the detection performance.

d: ARTIFICIAL INTELLIGENCE ANOMALY DETECTION

Artificial intelligence (AI) techniques for DoS detection in WSNs automates the intrusion detection process to limit the rate of human intervention. The intrusion detection process using AI can be categorized into traditional artificial intelligence (TAI) and computer intelligence (CI) [69]. The former use methods such as evolutionary computing, neural network and fuzzy set as classifiers for anomaly detection. The latter, on the other hand, is usually preferred to handle issue related to attack modification. CI is often used during the construction of intelligent detection model to automatically identify an anomaly in the network with high-accuracy. AI techniques require continuous learning to ensure new anomalies can be effectively detected.

Sun *et al.* [101] in their work combined cultural-algorithm and artificial-fish-swam-algorithm optimized back propagation (CA-AFSA-BP) with hierarchical structured adaboost algorithm, to enhance the detection rate of an integrated intrusion detection model in WSN. CA-AFSA-BP is a misuse detection technique that is deployed on the sink nodes. It is a dual evolutionary system consisting of communication protocol, belief space and population space. Adaboost, on the other hand, is used to construct two-pass classifier. The sink nodes, in this work, receives data from either the cluster heads or from outside. Due to the high dimension of network intrusion data, principal component analysis (PCA) is used to reduce the dimension of the system in order to reduce the volume of storage and bring down the rate of energy consumption. During intrusion detection, anomaly data is a small proportion of all the data, therefore, in the first level of detection, most of the normal data are ruled out leaving the few anomaly data for subsequent levels. The combination of both algorithms resulted into a relatively high detection rate and low false alarm.

Chen *et al.* [102] propose an IDS based on immune algorithm and SVM in WSN. The immune algorithm is used to pre-process the network data before classification, using SVM. Alrajeh *et al.* [103] propose an artificial neural network (ANN) to detect energy depletion attack that cause denial of service in a cluster-based WSN. ANN consist of four components; namely: input, weight, activation function and output. It is inspired by the nervous system, where specific neurons are activated by strong signals, which in turn generates an output signal to detect flooding attacks. The proposed technique utilizes an unsupervised back propagation, based on learning, where threshold is used as the activation function. The detection process is divided into three phases, namely: data gathering, training phase and result. Simulation results using NS-2 show a detection rate of 98% for flooding attacks and 95% for routing loop attacks.

Wang *et al.* [104] propose a multi-agent refined clustering method by deploying self-organising map (SOM) neural network and K-means clustering algorithm to detect intrusion in WSN. The multiple agents used consists of sentry agent, analysis agent, response agent and management agent. Each of these agents can either be independent of each other or cooperative. The sentry agents are deployed on each node and are responsible for monitoring all the sensor nodes activities. Data collected in the sentry node will be directed to the analysis agent for processing. Analysis agents are also located in each sensor nodes and responsible for receiving and analysing data from sentry node to determine if an intrusion has occurred. The response agents are located in the sensor nodes and are responsible for receiving the analysed results from the analysis agents. If an attack is detected, a response agent will be activated to take necessary measure. Finally, the management agent, installed in all the nodes, take part in network management. Among the tasks of the management agent is the maintaining, managing and harmonization of other agents.

An IDS that uses danger theory immune inspired technique has been proposed by Salmon *et al.* [53] to detect a denial of sleep attack, caused by a jamming interference. Danger theory uses a danger signal to identify an anomaly as the attacker that causes damage to the body, independent of being part of the body or not. Dendric cells (DCs) are used to process and detect different signals, such as danger signal, to classify the collected antigens into normal or anomalous. These cells are used as the control mechanism of AIS to determine if the WSN is under attack or not. The WSN in this work is made up of several sensor nodes and a base station. These sensor nodes can either be used as a DC (sensor-dc) or a lymph node (sensor-lymph). The logical architecture of the proposed IDS (see Fig. 7) consists of several components, such as, monitoring, context manger, intrusion detection manager, decision manager, rule base, parameter base and counter measures. These components are organised into four subunits, namely: Monitoring Environment (E-BOX), Storage (D-BOX), Intruder Detection (A-BOX) and Countermeasures (C-BOX). The sensor-dc houses the monitoring, intrusion detection manager, parameter base, context manager and the rule base component; while the counter measure component and the decision manager is hosted in the sensor-lymph. The monitoring environment subunit is responsible for capturing values of parameters, such as received signal strength information (RSSI), defined by the context manager, to represent input to proposed IDS to determine possible attack. The Intrusion detection manager is the central point of the architecture. It organises the tasks and coordinate actions and responses of other managers. The storage subunit stores collected parameter history, such as type of attack, attack parameter list and threshold value. Finally, the

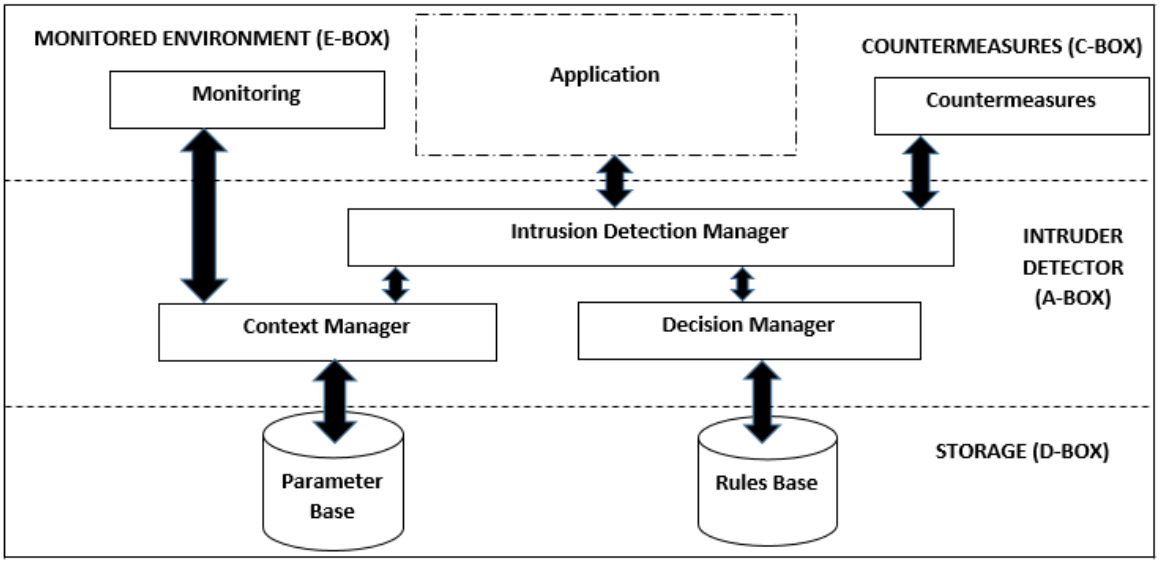

FIGURE 7. Logical architecture of danger theory immune-inspired IDS (adapted from [53]).

countermeasure subunit is responsible for mitigating the attacks identified. Experimental results, both in simulation and real sensor platform, show that the proposed IDS is efficient in both the detection of denial of sleep and energy consumption attack.

Gunasekaran and Periakaruppan [28] propose a table-based intrusion detection and swarm-based defence, herein called TIDSD, for predicting and preventing various DoS attacks in WSN. In this work, sensor nodes are arranged in a cluster form, with the cluster head initialized using an improved LEACH. The proposed method involves four stages, namely: predefinition of IDS, monitoring of member node (MN) by secondary cluster head (SCH), monitoring of SCH and MN by primary cluster head (PCH) and update of the monitored result in an isolated table of the base station. The swarm-based defence monitors the strength, flexibility, direct and indirect interactions between the sensor nodes while the table-based defence, on the other hand, identifies malicious behaviour that affects the channel, often referred to as faulty channel. A comparative analysis presented between the proposed TIDSD and other traditional IDS shows an efficient result with respect to energy consumption, rate of false alarm and DoS prediction and prevention accuracy.

A swam intelligence technique based on ant colony optimization has been proposed by Sreelaja and Pai [105] to detect sinkhole DoS attack in WSNs. The intrusion detection process has been divided into two phases. In the first phase, the ant colony optimization based attack detection (ACO-AD) algorithm, deployed in the sensor nodes of the WSNs, generates alert based on the quality of the link and the nodeids defined in the rule set. During the second phase, each alerted node sends a list of nodeids to the neighbouring alerted nodes to jointly agree and determine the attacker. During the transmission of the suspected list, the alerted node is signed using a key. A minimized Boolean expression, based on ant colony optimization technique, is used to generate a minimum amount of key to sign the suspect list. Furthermore, the ant colony optimization Boolean expression evolver sign generation algorithm is used to distribute keys to the alerted node to ensure the suspect list is signed. To identify the intruder, the alerted nodes use the received suspected list to determine the occurrence in each nodeid. The nodeid that has the highest count is identified as the intruder. Evaluation of the method suggests that this technique does not generate false positives and overcomes the demerit of SVM and NN for rule matching, using less storage.

Artificial intelligence anomaly detection techniques are adaptive in nature; in that they allow the training and testing of data instances in an incremental fashion. Therefore, techniques, such as neural network for unsupervised learning can effectively detect DoS attack in WSN. However, the issue of inadequate access to normal traffic data can affect the training process of the underlying algorithm; thus, affecting its efficiency. Furthermore, artificial intelligence methods are not easily scalable and can suffer from the issue of over-fitting during training.

3) SPECIFICATION BASED DETECTION

Specification based intrusion detection can be regarded as a form of anomaly detection without using user, group or data profiling [106]. It combines the aims of both misuse and anomaly detection approach to discover deviations from normal behaviour without the use of either machine learning or data mining techniques [8]. During attack detection in WSN, sets of specification and constraint are set manually to describe the normal behaviour of an event or network. The level of intrusion can, thereafter, be determined by measuring the rate at which it deviated from the specification. In deviance with anomaly based intrusion detection, specification based detection check for an anomalous performance

at the system level and indicate an intrusion when the system deviates from its normal operation [106]. This, therefore guarantees the deployment of a lightweight IDS for resource constraint devices, such as sensor nodes.

Farooqi *et al.* [107] propose an intrusion detection framework (IDF) in a distributed environment using a specification based detection approach in WSN. This approach detects intrusion through the collaboration of neighbouring nodes and works in two modes, namely: online prevention and offline detection mode. The online prevention mode ensures that legitimate nodes are protected from the malicious nodes in the network while the offline detection search for nodes that are being compromised by an adversary after installation. The proposed framework is distributed; therefore, the intrusion detection agent is installed in all the sensor nodes. The IDF works in a promiscuous mode by listening to traffic being transmitted in the network and decides whether to process and send to the next hop. Simulation implemented in C programming for a flat WSN shows that the proposed method achieves a high detection rate with low false positive. Furthermore, results show that a purely distributed approach is more effective in determining the actual condition of the network as against centralized distributed approach.

Tiwari *et al.* [108] in their work designed an intrusion detection system to mitigate against blackhole and selective forwarding attacks in WSN based on local information. This work uses a specification approach, where set of rules are defined to map behaviour of sensor nodes to either normal or abnormal. The rule used is based on the number of data dropped by a node during transmission. The tree approach is used to segment the network into clusters, with clusters partially overlapping. Cluster heads are selected and are in charge of the decision-making process to determine if the sending and receiving nodes in the cluster are legitimate or not. Watch dogs in the network are more powerful nodes and function to analyse transmitted data within their communication range. This approach optimizes the local information collected by the watch dogs into global information in the cluster head to reduce overhead in the network.

Krontiris *et al.* [109] propose an IDS to detect sinkhole attacks in WSNs using specification based approach in a realistic network that use MintRoute, one of the most used routing protocols in TinyOS. The deployed IDS has a distributed architecture with identical IDS agents running on each sensor node in the network. These IDS agents communicate with each other to make a joint decision on an intrusion event. The IDS agent has four functions, namely: network monitoring, intrusion detection, decision making and action. During network monitoring, each IDS agent listens in the network to capture and assess transmitted data within its listening range in real time. During the intrusion detection process, the IDS agents use a specification based approach to determine the behaviours that deviate from normal, using manually defined rules to detect an attack. During the decision-making stage, if an anomaly is detected by an IDS agent, a cooperative decision is taken by neighbouring nodes to reach a mutual conclusion. Finally, an action is taken by each node in response to the intrusion situation. Based on the described functions, the architecture of the IDS agent has been built around five conceptual modules, namely: local packet monitoring, local engine detection, cooperative detection engine, local response and the communication module.

Similar to their work in [109], a distributed lightweight intrusion detection technique has been proposed in [59] to detect blackhole and selective forwarding attacks using specification approach. In this work, only partial and local information available at the sensor node is available, therefore, neighbouring nodes collaborate and exchange information to take a joint intrusion decision.

Lemos *et al.* [110] propose a collaborative decentralized IDS in WSNs using a specification based approach to detect an attack. Special nodes called monitor nodes are used to watch over the entire network in a distributed fashion, with the intention of detecting an anomaly. The monitoring process is done by first specifying a normal node behaviour to detect an anomaly in a near real time fashion. The monitoring node stores sensed data in a fixed size buffer and applies the specified rule when the buffer is full. Rules defined in the IDS includes: interval rule, retransmission rule, integrity rule, delay rule, repetition rule, radio transmission range, valid destination rule, valid origin rule and jamming rule. Any rule violation higher than a predetermined threshold will result in an abnormal behaviour. To cater for component failure in the network, information from neighbouring monitoring nodes will be correlated to confirm the malicious node. The collaboration between monitoring nodes can either be a common monitor or supervisor monitor. Evaluation of the proposed method, using Sinalgo, shows that it is effective in reducing false positives during detection.

Specification based detection techniques, that detects DoS attack in WSNs, present a low false negative rate during attack detection. It only flags an anomaly when an irregular behaviour that deviates from the previously manually defined profile is detected. Furthermore, specification based detection is very effective as no training or profiling is needed. One notable disadvantage of specification based detection is the enormous time and rigorous effort required to generate a formal specification. Also, this technique cannot detect specially crafted malicious behaviours that do not violate the defined specification.

4) HYBRID BASED DETECTION

Hybrid based detection technique is achieved by combining both signature and anomaly based detection techniques, to use their complimentary features, to coexist and interact as one single entity [8]. Hybrid based detection technique make use of training based anomaly technique and signatures in the knowledge database to achieve a higher detection rate. The hybrid based detection technique differs from the earlier stated specification based detection technique, as the former combines the techniques of both signature and anomaly based while the latter combines the aims of the two techniques.

Yan *et al.* [111] in their work propose a hybrid IDS (HIDS) that combines anomaly and misuse detection in a cluster-based WSN to detect attacks. The proposed HIDS consists of three modules, namely: the anomaly detection module, the misuse detection module and the decision-making module. The anomaly based detection module acts like a filter to large packet records to distinguish between normal and anomaly packets. The misuse detection module uses a knowledge database of well-known attack behaviour through the supervised learning of back propagation network (BPN). The supervised PBN is used to learn the relationship between input and output to tune the corresponding weight. The proposed HIDS is deployed in the cluster head, due to its higher capacity, to detect attacks. Lastly, the output of both anomaly and misuse detection module is integrated in the decision-making module to determine whether an output is anomalous or not, and the type of attack. Experimental results using Matlab 7.1 and KDDCup '99 show a detection rate of 99.81%, false positive rate of 0.57% and accuracy of 99.75%.

An integrated IDS for heterogeneous cluster-based WSNs has been proposed by Wang *et al.* [112] by combining three individual IDSs, namely: Intelligent Hybrid IDS (IHIDS), HIDS and misuse IDS to provide a real-time packet analysis, to detect an attack and resist intrusion. These three separate IDSs are designed for the base station, cluster head and sensor node. For the base station, the IHIDS that can learn is proposed by combining the anomaly and misuse detection method, with the aim of achieving a high detection rate and low false positive rate. For the cluster heads, the HIDS, which has a similar detection model as IHIDS but without learning ability is proposed. Here, the objective of HIDS is to efficiently detect attacks with minimum recourses. HIDS ensures new attacks behaviour, that has been detected and classified in IHIDS, are retained. For sensor nodes, misuse IDS is proposed by using stored attack patterns to match and detect attacks in the network. Due to the limited resources of ordinary sensor nodes, when compared with cluster heads or base station, simple and fast detection methods are adopted. Experimental performance of the misuse detection, using BPN and KDDCup'99 dataset, shows a detection rate of 90.96%, false positive rate of 2.06% and accuracy of 99.75%. To further improve the result obtained, an Adaptive Resonance Theory (ART) was introduced to the IHIDS to perform learning and detection of new attacks simultaneously. This produced an improved accuracy rate to detect five types of attack.

A dynamic approach for IDS in WSNs has been proposed by Huo and Wang [113]. The Dynamic Intrusion Detection System(DIDS) consists of both misuse and anomaly detection and are deployed on selected sensor nodes in the network. Once any of the nodes that houses the IDS consumes 30% of overall battery after IDS is activated, the cluster will reconfigure and the IDS will be deployed in new nodes and new clusters. The DIDS was simulated in NS-2 and compared with static models in WSN. Results show that DIDS detection rate is 10% higher than its static counterpart with a range of 15m. Furthermore, DIDS can extend the lifetime of a network by an average of 8%.

Hai *et al.* [114] propose a hybrid lightweight IDS based on anomaly and misuse techniques to detect DoS attacks, such as selective forwarding, sinkhole and hello flooding in WSNs. The proposed IDS, consisting of both local and global agents, are deployed on every sensor node. The local agent is used to monitor the sensor nodes when sending and receiving data. The sensor nodes do not have any knowledge about malicious nodes initially, however, this is gradually constructed after the deployment of WSN to form a signature database. The cluster heads, thereafter, transmits the database created to all sensor nodes. The global agent, on the other hand, monitor the communication that takes place among neighbouring nodes within its radio range. The global agent contains pre-defined rules from neighbouring nodes to monitor the packets. Any anomaly detected from neighbouring nodes results into the creation and sending of an alert to the cluster heads. The cluster heads, in turn, receive alert and make decision on the suspicious node using a pre-defined threshold. Evaluation of the proposed IDS show a good and effective detection method that suits a resource constrained WSN.

Gerrigagoitia *et al.* [115] in their work propose a reputation and trust based IDS to detect possible malicious attacks in WSNs. The proposed distributed IDS is a combination of anomaly based and specification based techniques, where each node has an IDS that monitor local activities to detect an anomaly. Sedjelmaci and Feham [116] propose a hybrid IDS framework for clustered WSN for attack detection. The proposed framework combines an anomaly detection technique based on SVM and a misuse detection. The SVM is used to classify data into normal and anomaly, while the misuse detection technique contains a collection of known attack signatures. The hybrid method achieves a high detection rate with low false alarm, while the clustering algorithm reduces the overheads and limits the energy consumed during attack defence.

While hybrid detection techniques provide the advantages offered by both misuse (signature) and anomaly based (and sometimes specification based techniques), such as, high detection rates and low false alarm; they introduce high complexity and overheads to the system, when trying to get different algorithms to interoperate and function as one entity. A summary of the reviewed detection techniques is presented in Table 3.

VI. DISCUSSION

In recent times, the Internet of Things (IoT) technology has enabled the interconnection of billions of devices within the global network. These devices are therefore able to monitor, sense and interconnect inside the global and dynamic internet. WSN, as the sensing-actuation arm of IoT, has played a pivotal role in the actualization of IoT. WSN has presented IoT with new opportunities which are more integrated to our daily life. Smart city, smart home and smart grid are examples of IoT applications, where sensor nodes are deployed and

TABLE 3. Comparative summary of DoS defence techniques in WSN.

Technique	Efficiency	Adaptive	Overhead	Overfitting	Scalability issues
Signature based			✓		✓
Statistical	✓				
Machine learning	✓	✓	✓		
Data mining	✓				
AI	✓	✓		✓	✓
Specification based	✓				
Hybrid	✓	✓	✓		

used to obtain information to improve the quality of life and quality of experience. Furthermore, real-time and near real-time applications, such as, healthcare system, smart traffic light system and traffic flow maintenance system are applications supported by IoT through the deployment of sensor nodes. The availability of these sensor nodes is therefore key to the existence and functionality of the IoT technology. DoS has been identified as the main security challenge to availability [6], therefore this work has presented various DoS attacks and defence solutions in WSN.

In the preceding section, we discussed the different forms of DoS attacks that depletes the resources of sensor nodes in WSN, using a layered approach. The aim of the DoS attack is to send series of malformed packets towards the target node to overwhelm and consume its resources. If not curtailed, it can shut down the entire network to deny the sensing and monitoring function of the sensor nodes in WSN. From the reviewed works, most research efforts seem to be directed towards the last three layers (i.e. network, link and physical layer) as against the transport and application layer. The reason behind several reported cases of DoS attacks in the lower layer is because of the ease at which the attack is carried out. Often a times the attack does not attempt to exploit the vulnerability of WSN, rather, they direct malicious packets towards the direction of the target node to jam its signals or consume the energy of legitimate nodes. DoS attacks on the upper layer (i.e. transport and application layer), for example path-based attack [52] and TCP SYN flooding [117] have also been reported. These attacks, oftentimes exploit the system weakness or protocol vulnerabilities to perpetrate the attack. However, very few reported publications on upper layer DoS attack mitigation have been proposed in WSN.

The most common defence deployment location in WSN is the sensor nodes, thereafter, the cluster heads and lastly the base station (see Fig. 8). Sensor nodes IDS deployment presents a distributed method, where each node can detect a DoS attack in a fast and efficient way. The sensor node IDS deployment often serve as local agent to obtain local information from suspicious nodes to detect an attack. This deployment sometimes presents an inconclusive decision, due to the partial information available; therefore, it can either collaborate with IDS in other sensor nodes, cluster

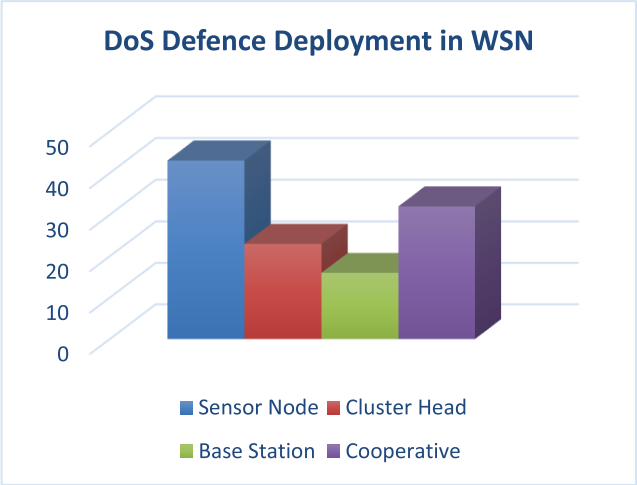

FIGURE 8. DoS defence deployment in WSN.

heads or base station to make a joint decision. The resource constraints of the sensor nodes can be a huge hindrance to the deployment of IDS, therefore, most IDSs deployed here are often lightweight. The cluster head, on the other hand, has been described to have a higher capacity when compared to the ordinary sensor nodes. IDS deployed here oversee the nodes in its cluster to detect an attack. IDS in cluster head can serve as a global agent that contains sets of predefined rules used to make decisions whether a sending node in the cluster is legitimate or not. The IDS deployment in cluster head can either solely oversee the entire WSN or collaborate with the sensor nodes or base station to form a cooperative approach. Lastly, the base station IDS deployment presents a centralised approach. Here, the IDS is deployed in the base station to take advantage of its enormous resources to monitor cluster heads within its coverage area to detect an attack. The centralised placement of the IDS in the base station conserves the energy resources of the sensor nodes, however, this approach can lead to a single point of failure.

Signature based techniques for DoS detection in WSN, from the reviewed works, seems to be dominant in the earlier suggested techniques, as compared to solutions proffered lately. It uses the signatures in its knowledge database to

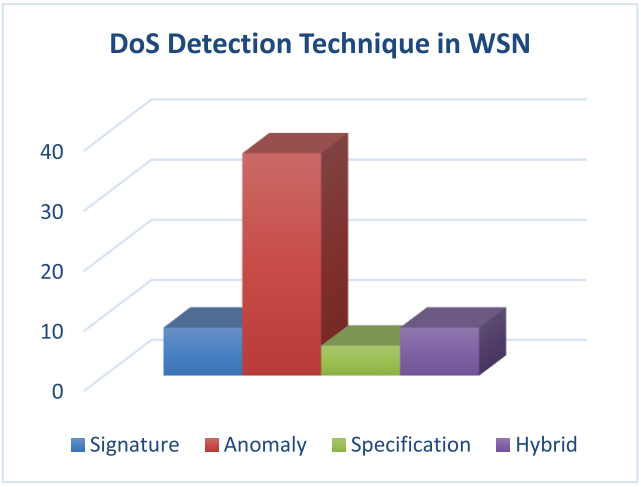

FIGURE 9. DoS detection techniques in WSN.

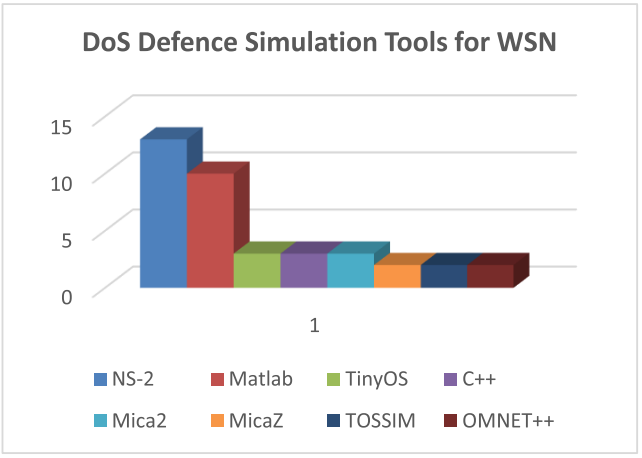

FIGURE 10. Simulation tools for evaluating proposed DoS techniques.

classify known DoS attack patterns. While this technique is effective for known DoS attack patterns, it is fast becoming irrelevant in today's threat landscape due to their inability to detect variation of known attack and unknown DoS attack signatures. The availability of open source DoS attack tools has made signature based detection techniques less effective, therefore, leading to a high false negative rate. Anomaly based detection technique in recent times, has shown to be increasingly popular in detecting DoS attacks in WSN. It presents a more efficient approach for detecting both unknown and derivative of known attacks patterns. This is achieved by modelling a normal traffic profile using techniques, such as statistical methods, data mining, machine learning and artificial intelligence. During the non-attack period in WSN, packet attributes are extracted to create a profile of normal behaviour. This is used during attack period to analyse transmitted traffic in the network to detect a DoS attack in the network. Another detection technique, which is seemingly similar to anomaly detection, is the specification based detection technique. Specification based detection guarantees a lightweight detection in deviance to anomaly based, by combining the aims of both misuse and anomaly detection without the use of either machine learning or data mining approach. The normal behavioural patterns in specification based detection technique are set manually, therefore, this can lead to classification error. Hybrid detection takes advantage of the complementary features of both signature and anomaly based techniques by integrating the duo to achieve a better detection rate. Some other hybrid techniques combine anomaly and specification based techniques to achieve a high detection with reduced overhead [115].

Figure 9 shows the summary of some existing DoS attack detection techniques between 2004 and 2017. It is observed that 64% of the proposed techniques are anomaly based while signature and hybrid based techniques, each make up 14%. Finally, specification detection technique constitutes only 8%. This further confirms the increasing popularity of anomaly detection technique.

To validate the proposed techniques and algorithms, real sensor platforms and experimental simulation tools have been deployed. Figure 10 depicts a chat that describes the different simulation tools used for the evaluation of proposed DoS detection techniques in WSN. It was observed that a large percentage of authors used NS-2, keenly followed by Matlab. Other notable simulation platform and tools are TinyOS, C++ based, Mica2, MicaZ, TOSSIM and OMNET++. Furthermore, during the evaluation phase of DoS defence, both synthetic and real-life datasets can be used for training and testing. An example of a real-life dataset is the Intel Berkeley Research Laboratory dataset [118] while WSN-DS [1] is an example of specialized synthetic DoS dataset. The availability of specialized DoS dataset for WSN remains a lingering challenge; this is evident as authors still rely on KDD CUP'99 dataset and its improved version, NSL-KDD, for evaluation. The KDD CUP '99 contains several flaws, such as the existence of large redundant and repeated records, which can produce a biased result towards frequently occurring records. Additionally, only few publicly representative labelled DoS datasets are currently available for use today by researcher.

The performance measure of different proposed techniques can be used to determine its efficiency and accuracy [119]. To determine the detection accuracy, a measure of the true positive (TP), true negative (TN), false positive (FP) and the false negative (FN) must be considered [120]. TP is said to be the percentage of correctly classified attacks while TN is the amount of normal test instance classified correctly. FP, also known as false alarm rate, is the amount of normal instance misclassified as an attack while FN is the percentage of attack instance misclassified as normal.

Proposed DoS defence techniques in WSN requires a high detection rate and low false alarm, therefore, the performance measure can be determined by comparing the accuracy, detection rate, false alarm rate and detection time.

TABLE 4. Summary of some existing DoS attack detection techniques, deployments and simulators in WSN.

Year	Reference	Detection technique				Defence Deployment				Simulator
		Signature	Anomaly	Specification	Hybrid	Sensor node	Cluster head	Base station	Cooperative	
2004	[70]	✓				✓				NS-2
2005	[68]	✓				✓				C++ designed
	[82]		✓			✓				N/A
2006	[64]		✓						✓	N/A
2007	[109]			✓		✓			✓	TinyOS
	[57]		✓						✓	NS-2
	[58]		✓					✓		OMNET++
	[59]			✓		✓			✓	N/A
	[114]				✓	✓	✓		✓	N/A
2008	[63]		✓			✓				NS-2
	[67]	✓				✓				N/A
	[113]				✓	✓				NS-2
2009	[104]		✓			✓		✓	✓	N/A
	[108]			✓		✓	✓		✓	N/A
	[111]				✓		✓			Matlab
2010	[34]	✓				✓			✓	TinyOS/TOSSIM
	[47]	✓				✓				OPNET Modeler
	[55]				✓		✓			Matlab
	[65]	✓				✓	✓	✓	✓	Telos and MICAz
	[78]		✓							N/A
	[87]		✓							N/A
	[90]		✓			✓	✓			Matlab
	[99]		✓			✓				C++ designed
	[110]			✓		✓			✓	Sinalgo
2011	[60]		✓			✓			✓	C based programme
	[81]		✓			✓	✓		✓	N/A
	[112]				✓	✓	✓	✓	✓	Matlab
	[116]				✓	✓	✓		✓	N/A
2012	[45]		✓			✓	✓		✓	N/A
	[56]				✓		✓	✓		N/A
	[76]		✓			✓				N/A
	[115]				✓	✓			✓	N/A
2013	[53]		✓			✓			✓	MICAz and TOSSIM
	[54]		✓					✓		NS-2
	[71]	✓					✓			C++ designed
	[77]		✓			✓			✓	MICA2
	[79]		✓			✓	✓	✓	✓	N/A
	[80]		✓			✓				NS-2
	[94]		✓			✓		✓	✓	NS-3
	[97]		✓			✓	✓		✓	Matlab
	[107]			✓		✓			✓	C based programme
2014	[27]		✓			✓				GAINZ/TinyOS
	[61]		✓				✓	✓	✓	NS-2
	[88]		✓			✓				Matlab
	[91]		✓				✓	✓	✓	NS-2
	[96]		✓				✓	✓	✓	Matlab
	[98]		✓			✓				NS-2
	[103]		✓			✓	✓		✓	NS-2
	[105]		✓			✓			✓	N/A
	[86]		✓			✓		✓	✓	OMNET++
2015	[72]	✓						✓		NS-2
	[89]		✓			✓	✓		✓	Mica2Dot
	[100]		✓			✓	✓	✓	✓	Matlab
	[101]		✓			✓	✓	✓	✓	Matlab
	[84]		✓			✓				NS-2
	[85]		✓			✓				Matlab
2017	[28]		✓				✓	✓		NS-2
	[83]		✓			✓	✓		✓	Mica2

Classification accuracy: Classification accuracy is defined as the percentage of data that are correctly defined from the total set. This can be represented by the situation of TP and TN. The classification accuracy of a proposed technique can be determined by:

$$\mathrm{CA} = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%$$

Detection rate: The detection rate of a classifier can be determined by using a confusion matrix. This is can be computed using the formula:

$$\mathrm{DR} = \frac{TP}{TP + FN} \times 100\%$$

False alarm rate: The false alarm rate is the percentage of normal data instance that has been misclassified as an attack. This can be determined by using the formula:

$$\mathrm{FAR} = \frac{FP}{FP + TN} \times 100\%$$

Detection time: This is the time it takes a classification technique to identify an attack packet during detection. A good detection technique is characterized by a short detection time. Table 4 summarises some of the existing DoS attack detection techniques, deployment location and the simulators in WSNs.

A. DRAWBACKS ON EXISTING PROPOSED METHODS

Despite the amount of research work that has been done on the defence of WSN against DoS attacks, there still exist some challenges that needs to be addressed. For example, most of the proposed techniques target a specific type on DoS attack directed towards a particular layer of the WSN, without paying cognisance to other layers. Contemporary online DoS attack tools are now open source and are capable of launching different types of DoS attacks to target different layers of the WSN. Therefore, a cross-layer IDS that can detect different forms of DoS attacks on different layers of the WSN will be essential.

Most of the reviewed work did not provide detailed experimental simulation of their proposed techniques (see Table 4). Furthermore, the lack of adequate real network traces has made the evaluation of proposed detection techniques difficult to analyse. Therefore, for proper training and evaluation, more attention should be channelled towards the production of labelled dataset with optimal features, in line with the current DoS attack pattern in WSN environment. This will ensure that an up-to-date dataset that are representative of the current DoS attack patterns are available for use.

The energy constraint of sensor nodes means that the proposed IDS must be lightweight for it to achieve its intended purpose. From the reviewed work, anomaly based detection techniques are the most deployed, and contains extensive IDS mechanism (such as data mining and artificial intelligence), therefore, a thorough functionality test must be carried out to guarantee its efficiency and suitability in WSN environment. This is essential because, sensor node deployment appears to be the most common deployment location that houses local IDS agent to provide on the spot detection, without the need to consult the cluster head and the base station.

The WSN structure will determine where IDS deployment will be most efficient in the network, therefore, this must be considered during DoS attack detection. For example, in a flat based topology, all sensor nodes are assumed to have the same capacity aside from the base station, therefore, sensor node deployment might be the most efficient in such instance. For a cluster-based topology, it is assumed that cluster heads are slightly of higher capacity, therefore, deploying IDS on the cluster heads will efficiently monitor cluster members in the network with less overhead. The hierarchical based topology is made up of both tree based and cluster-based network structure, therefore, proposing a satisfactory IDS location is non-trivial. However, a distributed and cooperative approach will provide a good trade-off.

VII. CONCLUSION AND FUTURE RESEARCH

DoS attack, in its different forms, is detrimental to the availability of resources and services of WSN. It disrupts the monitoring and sensing function of WSN by directing malformed packets towards the target node to deplete its energy and resources. In this paper, we first present the areas where WSN can be deployed, such as, terrestrial, underground, underwater, mobile and multimedia. The three-main network structure of WSN; flat-based, cluster-based and hierarchical-based network topology was also discussed before presenting a taxonomy of the different forms of DoS attacks targeting different layers of the WSN. A corresponding taxonomy was also presented for DoS defence in WSN, by categorizing the proposed approaches according to the technique used, defence network structure and their deployment location. A comparative summary of the different defence techniques was presented together with the different IDS deployment location, which is dependent on the network structure. Anomaly based detection and sensor node IDS deployment were identified as the most popular detection technique and deployment location proposed. Finally, the drawbacks of suggested techniques were highlighted and possible solutions was proposed.

DoS detection in WSN still presents some lingering challenges that needs to be addressed, which has been highlighted in the discussion section. For example, the need for a cross layer defence technique that can detect a cross section of DoS attacks in WSN, regardless of the targeted layer.

The physical layer jamming attack, that sends series of malicious signals to interfere with normal transmission, is one of the most catastrophic DoS attacks in WSN. The ease at which the jamming attack is perpetrated is a major concern, as no special hardware or software is needed. The attacker only passively listens to the open wireless medium and transmits its malicious signal on the same frequency channel to cause a collusion. Detecting a jamming attack is not trivial, as some deployed techniques misclassify packet failures caused by weak radio links and interference to jamming attacks to create a false alarm situation. Some other techniques proposed have relied on features like received ambient signal strength, packet-delivery-ratio, carrier sensing time, bad packet ratio and energy consumption amount. Common intrusion prevention schemes such as frequency hopping, spatial retreats are however beyond the capabilities of the current sensor nodes. Some sophisticated jamming attack that delay or interrupt alarm notification during DoS jamming attack detection has also been discussed. Even though

some approaches to detect both short and long term DoS jamming attack has been suggested, detecting a jamming attack that can dynamically change its attack pattern remains a challenge.

Furthermore, there is need for a thorough study on the deployment location of proposed IDSs and its effect on energy consumption in WSN. Effort should also be channelled into producing label dataset that is up-to-date and representative of the current DoS attack patterns in a WSN environment.

ACKNOWLEDGEMENTS

The views and opinions expressed in this article are those of the authors alone and not the organizations with whom the authors are or have been associated. The authors would like to thank the Editor-in-Chief, Associate Editor, and the anonymous reviewers for providing constructive criticism and generous feedback. Despite their invaluable assistance, any errors remaining in this paper are solely attributed to the authors.

REFERENCES

[1] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *J. Sensors*, vol. 2016, Aug. 2016, Art. no. 4731953.

[2] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in wireless sensor networks: A survey," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 1022–1034, 2012.

[3] R. E. Mohemed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Energy-efficient routing protocols for solving energy hole problem in wireless sensor networks," *Comput. Netw.*, vol. 114, pp. 51–66, Feb. 2017.

[4] X. Xu, K. Gao, X. Zheng, and T. Zhao, "A zero-sum game theoretic framework for jamming detection and avoidance in wireless sensor networks," in *Proc. Int. Conf. Comput. Sci. Inf. Process. (CSIP)*, Aug. 2012, pp. 265–270.

[5] 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.

[6] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *J. Netw. Comput. Appl.*, vol. 67, pp. 147–165, May 2016.

[7] A. D. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. 2004, pp. 739–763.

[8] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1223–1237, 3rd Quart., 2013.

[9] 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, 1st Quart., 2014.

[10] X. Huang, M. Ahmed, and D. Sharma, "Protecting from Inside Attacks in Wireless Sensor Networks," in *Proc. IEEE 9th Int. Conf. Depend., Auto. Secure Comput. (DASC)*, Dec. 2011, pp. 186–191.

[11] O. O. Ogundile and A. S. Alfa, "A survey on an energy-efficient and energy-balanced routing protocol for wireless sensor networks," *Sensors*, vol. 17, no. 5, p. 1084, 2017.

[12] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Netw.*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[13] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[14] I. F. Akyildiz and E. P. Stuntebeck, "Wireless underground sensor networks: Research challenges," *Ad Hoc Netw.*, vol. 4, no. 6, pp. 669–686, Nov. 2006.

[15] J. Heidemann, Y. Li, A. Syed, J. Wills, and W. Ye, "Underwater sensor networking: Research challenges and potential applications," USC/Inf. Sci. Inst., Marina del Rey, CA, USA, Tech. Rep. ISI-TR-2005-603, 2005.

[16] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Comput. Netw.*, vol. 51, no. 4, pp. 921–960, Mar. 2007.

[17] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, 2012.

[18] Q. Mamun, "A qualitative comparison of different logical topologies for wireless sensor networks," *Sensors*, vol. 12, no. 11, pp. 14887–14913, 2012.

[19] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. Choo, and M. Dlodlo, "From cloud to fog computing: A review and a conceptual live VM migration framework," *IEEE Access*, vol. 5, pp. 8284–8300, 2017.

[20] E. Stavrou and A. Pitsillides, "A survey on secure multipath routing protocols in WSNs," *Comput. Netw.*, vol. 54, no. 13, pp. 2215–2238, 2010.

[21] M. Al Ameen and K. Yoshigoe, "Security and attacks in wireless sensor networks," in *Wireless Technologies: Concepts, Methodologies, Tools and Applications*. Hershey, PA, USA: IGI Global, 2012, pp. 1811–1846.

[22] S. A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala, "Security in wireless sensor networks: Issues and challanges," in *Proc. IEEE Int. Conf. Space Sci. Commun. (IconSpace)*, Aug. 2013, pp. 356–360.

[23] J. Sen. (Nov. 2010). "A survey on wireless sensor network security." [Online]. Available: https://arxiv.org/abs/1011.1529

[24] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proc. 49th IEEE Conf. Decision Control (CDC)*, Dec. 2010, pp. 5967–5972.

[25] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," in *Foundations of Security Analysis and Design V*. Berlin, Germany: Springer, 2009, pp. 289–338.

[26] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," *Comput. Netw.*, vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[27] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on KNN classification algorithm in wireless sensor network," *J. Elect. Comput. Eng.*, vol. 2014, Jun. 2014, Art. no. 240217.

[28] M. Gunasekaran and S. Periakaruppan, "A hybrid protection approaches for denial of service (DoS) attacks in wireless sensor networks," *Int. J. Electron.*, vol. 104, no. 6, pp. 993–1007, 2017.

[29] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Change-point cloud DDoS detection using packet inter-arrival time," in *Proc. 8th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2016, pp. 204–209.

[30] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Trans. Mobile Comput.*, vol. 9, no. 7, pp. 941–954, Jul. 2010.

[31] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 318–332, Feb. 2013.

[32] K. Gill and S.-H. Yang, "A scheme for preventing denial of service attacks on wireless sensor networks," in *Proc. 35th Annu. Conf. IEEE Ind. Electron. (IECON)*, Nov. 2009, pp. 2603–2609.

[33] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 8, pp. 1119–1133, Aug. 2010.

[34] R. Rughiniş and L. Gheorghe, "Storm control mechanism in wireless sensor networks," in *Proc. 9th Roedunet Int. Conf. (RoEduNet)*, Jun. 2010, pp. 430–435.

[35] 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, Oct. 2017.

[36] M. Khatua and S. Misra, "CURD: Controllable reactive jamming detection in underwater sensor networks," *Pervasive Mobile Comput.*, vol. 13, pp. 203–220, Aug. 2014.

[37] H.-M. Sun, S.-P. Hsu, and C.-M. Chen, "Mobile jamming attack and its countermeasure in wireless sensor networks," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops (AINAW)*, vol. 1. May 2007, pp. 457–462.

[38] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *Int. J. Prod. Econ.*, vol. 172, pp. 76–94, 2016.

[39] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May 2006.
[40] Z. Benenson, P. M. Cholewinski, and F. C. Freiling, "Vulnerabilities and attacks in wireless sensor networks," in *Wireless Sensors Networks Security*. Amsterdam, The Netherlands: IOS Press, 2008, pp. 22–43.
[41] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes: Real-world physical attacks on wireless sensor networks," in *Proc. Int. Conf. Secur. Pervasive Comput.*, 2006, pp. 104–118.
[42] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, Jan./Mar. 2008.
[43] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.
[44] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 367–380, Jan. 2009.
[45] T. Bhattasali, R. Chaki, and S. Sanyal. (2012). "Sleep deprivation attack detection in wireless sensor network." [Online]. Available: https://arxiv.org/abs/1203.0231
[46] T.-G. Lupu, I. Rudas, M. Demiralp, and N. Mastorakis, "Main types of attacks in wireless sensor networks," in *Proc. WSEAS Int. Conf. Recent Adv. Comput. Eng.*, 2009, pp. 180–185.
[47] A. Baadache and A. Belmehdi. (2010). "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks." [Online]. Available: https://arxiv.org/abs/1002.1681
[48] H. Gao, R. Wu, M. Cao, and C. Zhang, "Detection and defense technology of blackhole attacks in wireless sensor network," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.*, 2014, pp. 601–610.
[49] W. Wang, S. Zhang, G. Duan, and H. Song, "Security in wireless sensor networks," in *Wireless Network Security*. Berlin, Germany: Springer, 2013, pp. 129–177.
[50] P. Li, L. Sun, X. Fu, and L. Ning, "Security in wireless sensor networks," in *Wireless Network Security*. Berlin, Germany: Springer, 2013, pp. 179–227.
[51] O. A. Osanaiye and M. Dlodlo, "TCP/IP header classification for detecting spoofed DDoS attack in cloud environment," in *Proc. Int. Conf. Comput. Tool (EUROCON)*, pp. 1–6, 2015.
[52] B. Li and L. Batten, "Using mobile agents to detect node compromise in path-based DoS attacks on wireless sensor networks," in *Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCom)*, Sep. 2007, pp. 2507–2510.
[53] H. M. Salmon *et al.*, "Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques," *Int. J. Wireless Inf. Netw.*, vol. 20, no. 1, pp. 39–66, 2013.
[54] D. E. Boubiche and A. Bilami, "A defense strategy against energy exhausting attacks in wireless sensor networks," *J. Emerg.*, vol. 5, no. 1, pp. 18–27, 2013.
[55] K. Yan, S. Wang, S. Wang, and C. Liu, "Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network," in *Proc. 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. (ICCSIT)*, vol. 1. Jul. 2010, pp. 114–118.
[56] M. S. I. Mamun and A. Kabir. (2012). "Hierarchical design based intrusion detection system for wireless ad hoc network." [Online]. Available: https://arxiv.org/abs/1208.3772
[57] D. Dallas, C. Leckie, and K. Ramamohanarao, "Hop-count monitoring: Detecting sinkhole attacks in wireless sensor networks," in *Proc. 15th IEEE Int. Conf. Netw. (ICON)*, Nov. 2007, pp. 176–181.
[58] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in *Proc. 3rd Int. Conf. Intell. Sensors, Netw. Inf. (ISSNIP)*, Dec. 2007, pp. 335–340.
[59] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proc. 13th Eur. Wireless Conf.*, 2007, pp. 1–10.
[60] Z. A. Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks," *Comput. Commun.*, vol. 34, no. 3, pp. 468–484, 2011.
[61] S. Shamshirband *et al.*, "Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 42, pp. 102–117, Jun. 2014.
[62] F. Amini, V. B. Mişic, and J. Mişic, "Intrusion detection in wireless sensor networks," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*. Boca Raton, FL, USA: CRC Press, 2007, p. 111.
[63] L. Huang and L. Liu, "Extended watchdog mechanism for wireless sensor networks," *J. Inf. Comput. Sci.*, vol. 3, no. 1, pp. 39–48, 2008.
[64] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2006, pp. 640–644.
[65] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," *IEEE Trans. Ind. Informat.*, vol. 6, no. 4, pp. 744–757, Nov. 2010.
[66] H.-J. Liao, C.-H. R. 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.
[67] Z. Yu and J. J. Tsai, "A framework of machine learning based intrusion detection for wireless sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous Trustworthy Comput. (SUTC)*, Jun. 2008, pp. 272–279.
[68] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proc. 1st ACM Int. Workshop Quality Service Secur. Wireless Mobile Netw.*, 2005, pp. 16–23.
[69] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, and A. Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique," *Eng. Appl. Artif. Intell.*, vol. 26, no. 9, pp. 2105–2127, 2013.
[70] F. Anjum, D. Subhadrabandhu, S. Sarkar, and R. Shetty, "On optimal placement of intrusion detection modules in sensor networks," in *Proc. 1st Int. Conf. Broadband Netw. BroadNets*, 2004, pp. 690–699.
[71] 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.
[72] F. Hidoussi, H. Toral-Cruz, D. E. Boubiche, K. Lakhtaria, A. Mihovska, and M. Voznak, "Centralized IDS based on misuse detection for cluster-based wireless sensors networks," *Wireless Pers. Commun.*, vol. 85, no. 1, pp. 207–224, 2015.
[73] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. 15, 2009.
[74] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 303–336, 1st Quart., 2014.
[75] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1, pp. 18–28, 2009.
[76] J.-W. Ho, M. Wright, and S. K. Das, "Distributed detection of mobile malicious node attacks in wireless sensor networks," *Ad Hoc Netw.*, vol. 10, no. 3, pp. 512–523, 2012.
[77] B. Sun, X. Shan, K. Wu, and Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks," *IEEE Syst. J.*, vol. 7, no. 1, pp. 13–25, Mar. 2013.
[78] A. G. Fragkiadakis, V. A. Siris, and N. Petroulakis, "Anomaly-based intrusion detection algorithms for wireless networks," in *Proc. WWIC*, 2010, pp. 192–203.
[79] J.-Y. Huang, I.-E. Liao, Y.-F. Chung, and K.-T. Chen, "Shielding wireless sensor network using Markovian intrusion detection system with attack pattern mining," *Inf. Sci.*, vol. 231, pp. 32–44, May 2013.
[80] P. Ballarini, L. Mokdad, and Q. Monnet, "Modeling tools for detecting DoS attacks in WSNs," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 420–436, 2013.
[81] F. Bao, R. Chen, M. Chang, and J.-H. Cho, "Trust-based intrusion detection in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2011, pp. 1–6.
[82] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, vol. 3. Aug. 2005, pp. 253–259.
[83] M. Xie, J. Hu, S. Guo, and A. Y. Zomaya, "Distributed segment-based anomaly detection with Kullback–Leibler divergence in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 101–110, Jan. 2017.
[84] M. Motamedi and N. Yazdani, "Detection of black hole attack in wireless sensor network using UAV," in *Proc. 7th Conf. Inf. Knowl. Technol. (IKT)*, May 2015, pp. 1–5.
[85] N. Assad, B. Elbhiri, M. A. Faqihi, M. Ouadou, and D. Aboutajdine, "Analysis of the deployment quality for intrusion detection in wireless sensor networks," *J. Comput. Netw. Commun.*, vol. 2015, Jan. 2015, Art. no. 812613.

[86] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 644–653, 2014.

[87] L. Ye, Z.-G. Qin, J. Wang, and J. Jin, "Anomaly event detection in temporal sensor network data of intelligent environments," in *Proc. 2nd Int. Conf. Comput. Eng. Technol. (ICCET)*, vol. 7. 2010, pp. V7-414–V7-420.

[88] A. Ghosal and S. Halder, "Tailor-made Gaussian distribution for intrusion detection in wireless sensor networks," in *Proc. Ubiquitous Intell. Comput. IEEE 11th Int. Conf. IEEE 11th Int. Conf. Auto. Trusted Comput., IEEE 14th Int. Conf. Scalable Comput. Commun. Assoc. Workshops (UTC-ATC-ScalCom)*, Dec. 2014, pp. 406–411.

[89] M. GhasemiGol, A. Ghaemi-Bafghi, M. H. Yaghmaee-Moghaddam, and H. Sadoghi-Yazdi, "Anomaly detection and foresight response strategy for wireless sensor networks," *Wireless Netw.*, vol. 21, no. 5, pp. 1425–1442, 2015.

[90] S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami, "Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 518–533, Sep. 2010.

[91] 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, Jun. 2014.

[92] S. Misra, K. I. Abraham, M. S. Obaidat, and P. V. Krishna, "LAID: A learning automata-based scheme for intrusion detection in wireless sensor networks," *Secur. Commun. Netw.*, vol. 2, no. 2, pp. 105–115, 2009.

[93] H. He, D. Zhang, X. Wang, M. Liu, W. Zhang, and J. Guo, "Multitask learning-based security event forecast methods for wireless sensor networks," *J. Sensors*, vol. 2016, Feb. 2016, Art. no. 6047023.

[94] A. Garofalo, C. Di Sarno, and V. Formicola, "Enhancing intrusion detection in wireless sensor networks through decision trees," in *Dependable Computing*. Berlin, Germany: Springer, 2013, pp. 1–15.

[95] M. Moshtaghi, S. Rajasegarar, C. Leckie, and S. Karunasekera, "Anomaly detection by clustering ellipsoids in wireless sensor networks," in *Proc. 5th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, 2009, pp. 331–336.

[96] S. Shamshirband, A. Amini, N. B. Anuar, M. L. M. Kiah, Y. W. Teh, and S. Furnell, "D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks," *Measurement*, vol. 55, pp. 212–226, Sep. 2014.

[97] D. Mansouri, L. Mokdad, J. Ben-Othman, and M. Ioualalen, "Detecting DoS attacks in WSN based on clustering technique," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 2214–2219.

[98] G. Kaur and M. Singh, "Detection of black hole in wireless sensor network based on data mining," in *Proc. 5th Int. Conf. Confluence Next Generat. Inf. Technol. Summit (Confluence)*, 2014, pp. 457–461.

[99] Z. Banković, J. M. Moya, Á. Araujo, D. Fraga, J. C. Vallejo, and J.-M. de Goyeneche, "Distributed intrusion detection system for wireless sensor networks based on a reputation system coupled with kernel self-organizing maps," *Integr. Comput.-Aided Eng.*, vol. 17, no. 2, pp. 87–102, 2010.

[100] S. Fouchal, D. Mansouri, L. Mokdad, and M. Ioualalen, "Recursive?clustering?based approach for denial of service (DoS) attacks in wireless sensors networks," *Int. J. Commun. Syst.*, vol. 28, no. 2, pp. 309–324, 2015.

[101] 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, p. e0139513, 2015.

[102] Y. S. Chen, Y. S. Qin, Y. G. Xiang, J. X. Zhong, and X. L. Jiao, "Intrusion detection system based on immune algorithm and support vector machine in wireless sensor network," in *Information and Automation*. Berlin, Germany: Springer, 2011, pp. 372–376.

[103] N. A. Alrajeh, S. Khan, J. L. Mauri, and J. Loo, "Artificial neural network based detection of energy exhaustion attacks in wireless sensor networks capable of energy harvesting," *Ad Hoc Sensor Wireless Netw.*, vol. 22, nos. 1–2, pp. 109–133, 2014.

[104] H.-B. Wang, Z. Yuan, and C.-D. Wang, "Intrusion detection for wireless sensor networks based on multi-agent and refined clustering," in *Proc. WRI Int. Conf. Commun. Mobile Comput. (CMC)*, vol. 3. 2009, pp. 450–454.

[105] N. K. Sreelaja and G. A. V. Pai, "Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks," *Appl. Soft Comput.*, vol. 19, pp. 68–79, Jun. 2014.

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

[107] A. H. Farooqi, F. A. Khan, J. Wang, and S. Lee, "A novel intrusion detection framework for wireless sensor networks," *Pers. Ubiquitous Comput.*, vol. 17, no. 5, pp. 907–919, 2013.

[108] M. Tiwari, K. V. Arya, R. Choudhari, and K. S. Choudhary, "Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local information," in *Proc. 4th Int. Conf. Comput. Sci. Converg. Inf. Technol. (ICCIT)*, 2009, pp. 824–828.

[109] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," in *Proc. Int. Symp. Algorithms Experim. Sensor Syst., Wireless Netw. Distrib. Robot.*, 2007, pp. 150–161.

[110] M. V. de Sousa Lemos, L. B. Leal, and R. H. Filho, "A new collaborative approach for intrusion detection system on wireless sensor networks," in *Novel Algorithms and Techniques in Telecommunications and Networking*. Dordrecht, The Netherlands: Springer, 2010, pp. 239–244.

[111] K. Q. Yan, S. C. Wang, and C. W. Liu, "A hybrid intrusion detection system of cluster-based wireless sensor networks," in *Proc. Int. MultiConf. Eng. Comput. Sci.*, vol. 1. 2009, pp. 18–20.

[112] S.-S. Wang, K.-Q. Yan, S.-C. Wang, and C.-W. Liu, "An integrated intrusion detection system for cluster-based wireless sensor networks," *Expert Syst. Appl.*, vol. 38, no. 12, pp. 15234–15243, 2011.

[113] G. Huo and X. Wang, "DIDS: A dynamic model of intrusion detection system in wireless sensor networks," in *Proc. Int. Conf. Inf. Autom. (ICIA)*, 2008, pp. 374–378.

[114] T. H. Hai, F. Khan, and E.-N. Huh, "Hybrid intrusion detection system for wireless sensor networks," in *Proc. Int. Conf. Comput. Sci. Appl.*, 2007, pp. 383–396.

[115] K. Gerrigagoitia, R. Uribeetxeberria, U. Zurutuza, and I. Arenaza, "Reputation-based intrusion detection system for wireless sensor networks," in *Proc. Complexity Eng. (COMPENG)*, 2012, pp. 1–5.

[116] H. Sedjelmaci and M. Feham. (2011). "Novel hybrid intrusion detection system for clustered wireless sensor network." [Online]. Available: https://arxiv.org/abs/1108.2656

[117] Z. He and T. Voigt, "Droplet: A new denial-of-service attack on low power wireless sensor networks," in *Proc. IEEE 10th Int. Conf. Mobile Ad-Hoc Sensor Syst. (MASS)*, Oct. 2013, pp. 542–550.

[118] M. A. Rassam, A. Zainal, and M. A. Maarof, "One-class principal component classifier for anomaly detection in wireless sensor network," in *Proc. 4th Int. Conf. Comput. Aspects Social Netw. (CASoN)*, 2012, pp. 271–276.

[119] O. Osanaiye, H. Cai, K.-K. R. Choo, A. Dehghantanha, Z. Xu, and M. Dlodlo, "Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 130, 2016.

[120] O. A. Osanaiye, "DDoS defence for service availability in cloud computing," Ph.D. dissertation, Dept. Elect. Eng., Univ. Cape Town, Cape Town, South Africa, 2016.

[121] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 2, pp. 70–159, 2nd Quart., 2010.

OPEYEMI A. OSANAIYE received the Bachelor's degree in electrical engineering from the University of Ilorin, Nigeria, in 2007, the Master's degree in telecommunications engineering from the University of Sunderland, U.K., in 2011, and the Ph.D. degree in electrical engineering from the University of Cape Town, Cape Town, South Africa, in 2016. He was a part time Lecturer with the Cape Peninsular University of Technology, Cape Town. He was with the University of South Australia as a Research Exchange Visitor from 2015 to 2016. He is currently a Lecturer with the Telecommunications Department, Federal University of Technology, and also a Post-Doctoral Research Fellow at the University of Pretoria, South Africa. His research interests include computer networks, cloud computing, wireless sensor network, fog computing, network security, voice over internet protocol technology, and cloud computing security. He is a registered COREN Member.

ATTAHIRU S. ALFA (M'00) is currently a Professor Emeritus with the Department of Electrical and Computer Engineering, University of Manitoba, and also a SARChI Chair Professor with the Department of Electrical, Electronic, and Computer Engineering, University of Pretoria. He has carried out applied research for Nortel Networks, Bell-Northern Research, TRLabs (now TRTech), Bell Canada, Winnipeg Regional Health Authority, Motorcoach Industries, and several other industries. He has authored the book, *Queueing Theory for Telecommunications: Discrete Time Modelling of a Single Node System* (Springer, 2010) and another one, *Applied Discrete Time Queueing Theory* (Springer, 2015). His research covers, but not limited to, the following areas: performance analysis and resource allocation in telecommunication systems, modeling of communication networks, queueing theory, optimization, the analysis of cognitive radio networks, modeling and analysis of wireless sensor networks, developing efficient decoding algorithms for LDPC codes, channel modeling, traffic estimation for the Internet, and cross layer analysis. He also involved in the application of queueing theory to other areas, such as transportation systems, manufacturing systems, and healthcare systems. He was the NSERC Chair for tele-traffic from 2004 to 2012.

GERHARD P. HANCKE (F'16) received the B.Sc., B.Eng. and M.Eng. degrees from the University of Stellenbosch, South Africa, and the D.Eng. degree from the University of Pretoria, South Africa, in 1983. He is currently with the University of Pretoria, where he is a Professor and a Coordinator of the Computer Engineering Program and the immediate past head of the Advanced Sensor Networks (ASN) Research Group, which has links with the ASN Group, Meraka Institute, and Council for Scientific and Industrial Research. He is recognized internationally as a pioneer and leading scholar in ASN research, especially aimed at industrial applications. He co-edited a textbook *Industrial Wireless Sensor Networks: Applications, Protocols, and Standards*, (2013), the first on the topic. He received the Larry K. Wilson Award in 2007, for inspiring membership development and services as a member of several regional and technical conferences worldwide. Apart from serving on several IEEE committees on section, regional, and board level, some as chair, he has been very active in the IEEE Technical Activities, in society administration, and conference organization on many levels, notably as the General Chair of the IEEE ISIE, INDIN, ICIT, and AFRICON. He initiated and co-edited the first special section on industrial wireless sensor networks in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS in 2009. His papers attracted high citation numbers in high impact journals.