Lightweight models for detection of denial-of-service attack in wireless sensor networks

Ademola P. Abidoye | Boniface Kabaso

Abstract
Wireless sensor networks (WSNs) are becoming more popular in recent times due to the availability of low cost, the short transmission range of sensor nodes and their easy deployment in different application areas; however, security is crucial for WSNs due to the nature of data they transmit in most cases in their locations. Sensor nodes transmit through an open medium and due to the short communication range of each sensor node, a node may need to transmit through many hops to a final destination. Denial-of-service (DoS) is one of the attacks that can be launched against WSNs to prevent legitimate nodes from transmitting/receiving data packets. Developing an attack detection and countermeasure system to mitigate the effect of DoS is not an easy task. This work proposes lightweight models for DoS attack detection in WSNs. We developed different lightweight models and algorithms for the detection and elimination of DoS in WSNs and experimented the same. The performance of data delivery ratio, delay, detection rate, energy consumption, and false-positive was carried out. The experimental results show that the proposed scheme achieved a high true-positive detection rate, low false-positive detection rate, energy-efficient, and high data reliability. Numerical examples are presented to further validate the effectiveness of the proposed scheme.

1 | INTRODUCTION

Wireless sensor networks (WSNs) have emerged as one of the recent technologies in the 21st century. WSNs consist of a set of interconnected independent devices called ‘sensor motes’ that can jointly measure changes such as temperature, pressure, noise level, humidity in the target area, and report to a data centre (base station) for further processing. The technology enables sensor nodes in WSNs to communicate with each other using wireless transceivers without pre-existing infrastructure. They provide distinctive opportunities for interaction between smart objects and their environment. They have been successfully used in many areas including smart parking, logistical and industrial applications, environmental ecological applications [1]. A typical sensor node is a small size, equipped with a smart sensor, a small processor, a short-range transceiver, with small batteries. The nodes exchange data packets among themselves to build a wide view of the target area [2].

Data routing plays a major role in WSNs. It is the process for transmitting sensed data from source nodes to a data centre through different routes in a network. Due to the unique characteristics of WSNs, routing security is an important research area. For the WSNs to remain functional for a longer period, resilience to sensor node failure is necessary. Thus, the method by which WSNs could fail is an attack on sensor nodes [3]. Many routing protocols have been proposed in the literature, but only a few considered security as a main challenge for WSNs [4–6]. Thus, security in WSNs should be considered as an important issue due to sensitive information they transmit over a wireless medium. Similar to wired network architecture, WSNs are organised in layers based on the Open Systems Interconnection (OSI) model [7, 8]. Figure 1 shows a conceptual framework used to describe network connectivity in seven distinctive layers. These include the Physical layer, Data link-layer, Network layer, Transport layer, and Application layer.

In this article, we are considering only attacks at the network layer because the major function of this layer is routing [9]. Wide application areas of WSNs, mode of deployment, communication medium, the lack of pre-existing infrastructure, all these make them vulnerable to different kinds of attacks in which...
denial-of-service (DoS) attacks are recognized as one of the most serious threats in WSNs [10, 11]. It can initiate other malicious activities such as spoofing, flooding, wormhole, and sinkhole attacks [12]. DoS attack refers to malicious attempts to prevent legitimate sensor nodes from receiving/transmitting sensed data by depleting the energy of sensor nodes or obstructing their communication path [13]. It aims to thwart legitimate sensor nodes from functioning efficiently either temporarily or indefinitely. It saturates the victims with unnecessary communication requests and due to this, the victim would not be able to communicate with other legitimate nodes at all or responds very slowly, vanishing its effectiveness. DoS attack is like traffic congestion on the highway, preventing road users from arriving at its desired destination. The attacks occur majorly in the form of (i) interruption that is a breakdown of a communication link, (ii) confiscation—unauthorized access of information stored on the sensor nodes, (iii) alteration—change of data packets by unapproved access, and iv) fabrication—the inclusion of false information by the compromised sensor nodes within the WSNs [10, 14].

1.1 | Motivation

Applications of WSNs have increased exponentially over the past decades. Similarly, there has been an increase in network attacks. DoS attacks are one of the WSN attacks; their main aim is to overwhelm the target sensor nodes with bogus data, drain their limited energy, and create energy holes within the network. Thus, operations of the WSNs will be affected and experience service disruption. There is a need to prevent/remove these attacks in the network. This work proposes a secure lightweight scheme applied to sensor nodes in the network.

1.2 | Problem statement

Next-generation sensor networks are predicted to be deployed in the Internet of Things (IoT) using heterogeneous sensor fabrics and following a service architecture where the sensor nodes/motes are equipped with different sensing, identification, and communication capabilities [15, 16]. They are tasked to deliver different services to different users anytime, anywhere, and using anything to reach some of the areas of our lives that we could not fathom without the advances made in the sensor technology. Attackers exploit vulnerabilities of sensor nodes to launch attacks and compromise legitimate sensor nodes in WSNs. All compromised sensor nodes actively participate in the attack process, generate a large amount of useless data, and forward them towards the nodes [17]. As a result, it is important to prevent the attacks by having a secure deployable protection scheme applied to sensor nodes in WSNs. This work presents a lightweight, efficient, and scalable scheme for the detection of DoS attacks in WSNs. The objective of this article is to develop an effective algorithm and models to allow sensor nodes to communicate over the networks and detect DoS attacks as soon as possible and remove the attacks and also to minimise the impact of the false-positive attacks in WSNs.

1.3 | Contributions

Considering the limited power source and resource-constrained sensor nodes, we propose lightweight security models for the detection of DoS attacks (LSDoS) in cluster-based WSNs. The scheme provides trust network management techniques. The main aim of using ‘trust’ is to ascertain that the WSNs work efficiently by detecting and removing compromised sensor nodes in the networks. The scheme assesses the current trust values of all the cluster heads in the data centre to monitor a cluster head’s behaviours in the network.

In addition, we develop a model that correctly classifies sensed data in the network into three categories to minimise false-positive rates and false-negative rates.

Finally, we develop models for quality of service (QoS) to increase the security of applications in WSNs. The following factors are considered: availability, reliability, and serviceability (ARS) to ensure that the integrity of data transmitted during network operation is maintained.

To the best of our knowledge, all these approaches used in this article have not been used together to detect and prevent DoS attacks in WSNs in the previous research works.

The rest of this paper is organised as follows. Section 2 discusses related work. Section 4 presents performance evaluation and discussion of results. Finally, conclusion and future work are discussed in Section 5.
2 RELATED WORK

DoS attacks is now one of the major threats in WSNs. The main aim of DoS attacks is to deplete the limited energy of sensor nodes and waste communication bandwidth. Thus, the attacks slowly reduce the general performance as well as the functionality of the WSNs. In recent years, many approaches have been developed in the literature to prevent DoS attacks in WSNs. Table 1 presents the comparison for DoS attacks.

Mansouri et al. [18] proposed the detection of DoS attacks in WSNs based on clustering. The method is divided into two phases: control sensor nodes election and detection and prevention of compromised sensor nodes. The authors recursively applied Low Energy Algorithm Adaptive Clustering Hierarchy (LEACH) algorithm [19] for selecting cluster heads which are considered as control sensor nodes. The numerical results obtained show that the approach gives significant results in terms of detection rate and time detection.

However, this approach may not be able to detect the attackers if their number is in a range of two digits (i.e. 10 upward).

Fouchal et al. [20] proposed a recursive-clustering-based approach for DoS attacks in WSNs. The approach recursively clusters sensor nodes until a required granularity is achieved. The authors developed a Fast and Flexible Unsupervised Clustering Algorithm (FFUCA) based on ultrametric properties. The main principle of FFUCA is deducing the behaviour (i.e. cluster seeds and thresholds) of the sensor nodes according to a given proximity criterion and aggregating member sensor nodes in clusters. Performance evaluation shows that the proposed scheme can detect more false alerts than compared protocols. However, this approach is not mathematically proved.

Securing WSNs from DoS attacks using artificial intelligence and the CLIPS expert system tool is proposed in [21]. The authors developed a system that would protect a WSN from DoS attacks after one or more sensor nodes on the network have been compromised and reprogrammed by an attacker. This scheme eliminates the need to rely on tamper-proof packaging to protect sensitive data and cryptographic keys which are stored on sensor nodes. With the proposed method, if an attacker can obtain the keys and used them to send false routing information, the network would be able to detect such compromised sensor nodes by using artificial intelligence and an expert system developed. However, the implementation of this approach was not carried out. It is difficult to ascertain the efficiency of this approach compared to previous approaches.

Zhang et al. [22] proposed testing and defending methods against DoS attack in state estimation (MADoS). The approach focussed on how wireless sensor and actuator networks (WSAN) can discover if it is below. They formulated the detection problem as a hypothesis testing problem and only if the statistics of the communication channel are known a priori. In addition, they proposed two defence countermeasures. The first uses a secured packet coding approach to partly compensate for the previous packet loss, and the second uses the sensor’s transmission power to resist the jamming effect brought by the DoS attack. However, this is not compared with previous related work and only three test results were obtained, indicating that the proposed scheme may not be efficient.

Osainye et al. [23] present DoS for resource availability in WSNs, deployment location, and possible countermeasures. The authors described a taxonomy of DoS attacks at different layers of the WSNs. They further categorised the network structure of DoS in WSNs into three, namely hierarchical defence, standalone defence, and distributed defence. However, the results of the research work are not enough to support the proposed approach.

Dhuria and Sachdeva [3] proposed the detection and prevention of DoS attacks in WSNs. The authors introduced two methods—a lightweight two-way authentication method to prevent the majority of DoS attacks and traffic analysis methods for data filtering to detect and prevent DoS attacks in WSNs. Simulation results show that the proposed scheme can detect and prevent DoS attacks in WSNs. However, the authors did not compare the proposed scheme with other related work to prove the effectiveness of the proposed methods.

Al Al-issa et al. [24] proposed machine learning techniques to detect DoS attacks in WSNs. The authors used LEACH technique to collect large data sets representing WSN features in different attacking scenarios. The data sets used contain regular profiles and several DoS attack scenarios in WSNs. The results of the experiment show that techniques achieved a higher true-positive rate of 99.86% and a lower false-positive rate of 0.05%. This approach is not scalable.

3 PROPOSED SYSTEM ARCHITECTURE

Network architecture for our proposed scheme consists of sensor nodes SNs (n) and a base station (BS). Considering the limited power source of each sensor node in WSNs, the network is divided into finite $K$ clusters (i.e. $C_k$ such that $k = 1, 2, ..., K$) in order to minimise energy consumption during data transmission. Each cluster consists of a cluster head (CH) and member nodes. Member nodes with communication radius $d$ less than or equal to the distance threshold value do [25] belong to the same cluster. Thus, every sensor node in the network could meet the free space model which can efficiently minimise energy consumption. The CHs are selected from sensor nodes of each cluster in order to ensure a better energy balance while maintaining the best detection coverage. The average number of sensor nodes per cluster and a finite number of CHs (i.e. $CH_k$ such that $k = 1, 2, ..., K$) in the network is obtained using Equation (1). Assuming that a CH belongs to a cluster in a network.

$$\sum_{k=1}^{K} \left( \frac{m}{\sum_{i=1}^{n} (n_i)} \right) C_k$$

(1)
A method in [26] is used to partition the network into different clusters and for uniform distribution of CHs within the network as shown in Figure 2. The group leaders, CHs, are responsible for managing the communication in clusters while SNs are the members of clusters. Their major responsibility is to detect and respond to some type of input from the physical environment.

Data transmission between the $n_S$ and base station is divided into the intra-cluster transmission and inter-cluster data transmissions.

Intra-cluster transmission: During intra-cluster transmission, $n_S$ only transmit to their corresponding CHs. Energy dissipation by the CH is linearly dependent on the number of $n_S$ in each cluster.

Inter-cluster transmission: During inter-cluster transmission, CHs transmit the aggregated data received from member nodes to the base station for further analysis and processing.

Thus, due to the broadcast nature of the transmission medium of $n_S$, they are often placed in a hostile or dangerous environment that makes them vulnerable to various attacks. We are more interested in DoS attacks because of wide application areas of WSNs and their limited power source. The aims of DoS attacks are:

- to drain limited energy of sensor nodes;
- to prevent legitimate sensor nodes from receiving sensor data from sender nodes;
- to disrupt the communication of two sensor nodes by using all the bandwidth that their connection has to offer.

### 3.1 Adversary nodes

The adversary nodes are set of malicious nodes in a network to cause loss of data either directly or through other means with the aim of launching a DoS attack [27]. These sets of nodes can be classified into the following:

(a) **Legitimate nodes**: These are normal sensor nodes in which their main responsibilities have not been compromised by malicious nodes or other entities. The main functions of the normal node are to sense environmental data and data transmission. The legitimate nodes of the network include relay nodes, cluster heads, and base station.

(b) **Compromised nodes**: These are legitimate sensor nodes but their main responsibilities have been taken over by the attackers to prevent them from the normal transmission. Some nodes that have been compromised in the network are shown in Figure 2.

(c) **Injected sensor nodes**: These types of nodes may be either legitimate nodes with normal sensing capabilities or more powerful nodes with high processing power.

(d) **A laptop-class adversary**: This type of adversary can broadcast with high transmission power and a battery capacity that can sustain the node for a longer period as compared to normal nodes [28].

Sensor nodes transmit through a wireless medium; this makes legitimate nodes vulnerable to DoS attacks launched by the adversarial nodes in the networks. The adversary node launches the attack by initiating the malicious node in the network to transmit useless data packets from several ends of the network towards the target nodes to disrupt data transmission of normal nodes within the network. Abbreviations and meanings of some of the terms used in this work are contained in 2.

### 3.2 Assumptions

The following are assumed for this work:

- All communication links between the $n_S$ and their corresponding CHs are bi-directional
- $n_S$ are randomly distributed within the network area
- If a $n_i$ is compromised, its data is also compromised
- Each cluster $C_k$ maintains a CH, $CH_k$, and member nodes $n_S$
- SNs communicate with a CH within fixed radio range
- Adversaries aim to disorder the communication of the entire network with DoS attacks
- The base station is located outside the network and has unlimited memory and power. Therefore, base station security issue is ignored
- Our security scheme is assumed to be a hierarchical structure.
### Table 2: Table of definitions

| Abbreviations | Meanings |
|---------------|----------|
| $C_k$         | Cluster $k$ |
| $n_i$         | Sensor node $i$ |
| $CH_k$        | Cluster head $k$ |
| $R_k(t)$      | Average number of sensed data received by a CH $k$ at time $t$ |
| $\mu$         | Factor ranges between 0 and 1 (i.e. $0 < \mu < 1$). It shows the vulnerability of the long-term average behaviour to the current traffic variation. |
| $\omega_k(t)$ | Number of sense data traffic received by a CH $k$ at time $t$ |
| $D_{k, \text{in}}(t)$ | Deviation of incoming traffic from the average at time $t$ |
| Subscript $\text{in}$ | Incoming traffic |
| $D_{A, \text{in}}$ | Deviation of incoming traffic from average, it is an indicator of attack |
| $\Phi$        | Measures the significant increase in bandwidth |
| $m$           | Average number of sensor nodes in a cluster |
| $T(n_N)$      | Trust value of total sensor nodes |
| $T_P(n_N)$    | Present trust value of $n_N$ |
| $T_H(n_N)$    | Past trust value of $n_N$ |
| $\beta_1$     | Factor for the present trust value |
| $\beta_2$     | Factor for the past trust value |
| $C$           | Victim nodes |
| $U$           | Target node |
| $Y$           | Adversary nodes |
| $m$           | Malicious node |
| $Z$           | Traffic flow |
| $a_i$         | Average time for data packet transmission and processing at node $i$ |
3.3 Analytical model of a sensor network experiencing a DoS attack

The analytical model of a WSN experiencing a DoS attack involves two types of network operation namely normal operation and attack operation.

**Normal operation:** The traffic flow in normal network operation is transmitted from the nodes to the data centre for processing and storage. During the transmission, a node may receive sensed data from member nodes within its transmission range. A CH node receives higher traffic flow both from normal nodes and malicious nodes in a network. We assume that every malicious node transmits data packet towards a target node $u$. Thus, in the presence of the DoS attack, the total data packet received by $u$ in a given period needs to be observed by the detection scheme which is expressed as follows.

$$
\beta^u = \sum_{i=1}^{CHs} \beta_{u,i} + \sum_{j=1}^{m} \beta_{u,j}
$$

where $\beta_{u,i}$ denotes the normal traffic flow from legitimate node $i$, and $\beta_{u,j}$ denotes the attack traffic from a malicious node $j$ in $Y$ to the legitimate node. If the average time for data packet transmission and processing at node $i$ is denoted by $a_i$ then the rate at which the data packet arrives at $u$ is expressed as follows.

$$
\mathcal{F}_i = a_i \left( \sum_{s=1}^{CHs} \tau_{s,i} \beta_{s,i} + \sum_{j=1}^{m} \tau_{u,j} \beta_{u,j} \right)
$$

$\tau_{s,i}$ denotes traffic rate for a legitimate node, $\tau_{u,j}$ denotes traffic rate for the attack node.

**Attack operation:** This type of operation considers the entire data packets transmitted from malicious nodes towards a set of target sensor nodes in the network. The total data packets received at node $u$ is a collection of the individual data packet of both the normal node and the malicious node. Thus, a joint effort is required to detect malicious data packets that are transmitted towards the legitimate nodes in the network.

3.4 Network model

In a WSN, sensor nodes are deployed in a sensing region to measure changes in the area of interest and periodically transmit to the base station through the CHs. It is more preferable for sensor nodes to transmit through the CHs because it can not only significantly minimise the energy consumption of sensor nodes but can also effectively minimise the signal propagation and channel fading effects associated with long-distance transmission [29–31].

We model the WSNs with a base station BS as a graph $G(N \cup BS, E)$, where $N$ corresponds to the set of sensor nodes randomly deployed in the network. $BS = n_{N+1} = z$ denotes the base station (destination node) and $E$ denotes the directional links between the nodes. Moreover, the first set deployment of sensor nodes is assumed to be normal (legitimate) nodes. The set of sensor nodes is represented as $N = \{S_0, n_1, n_2, \ldots, n_{N+1}\}$, where $S_0$ and $n_{N+1}$ are source and destination nodes respectively and $n_i$s = $i$s are sensor nodes of the network with added functionalities (relay sensory data, cluster heads for data aggregation and retransmission).

Victim nodes are expressed as a set of nodes $C = \{C_0, C_1, C_2, \ldots, C_{m-1}\}$, where $C \in N$, such that every target node $u$ of set $C$ is a legitimate node of the network, and $|C| = u \ll N$.

Thus, as new sensor nodes are added into the network due to the death or physical damage, some of these nodes may be compromised and become malicious nodes. Adversary nodes, $Y$, are set of malicious nodes in the network and expressed as follows.

$$Y = \{Y_0, Y_1, Y_2, \ldots, Y_{m-1}\}, \text{ where } |Y| = m \ll N.
$$

After deployment of sensor nodes, the BS generates unique IDs and sends them to all the nodes in the network. Each sensor node stores its ID and routing information of the nearest neighbouring node in its tabu (memory). The tabu contains node’s ID, location of the neighbouring node, and hop count. Sensor nodes in each cluster transmit their readings to the CH; the CHs in the network aggregate the readings, perform pre-processing on the received data and transmit the aggregated data to the base station for further processing.

Based on this mode of data transmission, end-to-end sensed data transmission is susceptible to DoS attacks.

The following attributes exist for each path between sensor nodes $n_i$ and $n_j$.

- **Transmission rate factor** $TR_{ij}(t)$ denotes the rate at which sensed data is being transmitted from node $n_i$ to node $n_j$ over a period of time $t$.

- **Data transmission** $DT_{ij}(t)$ denotes the amount of sensed data transmitted from node $n_i$ to node $n_j$ at time $t$. It is assumed to be the same for all legitimate sensor nodes.

- **Estimated value** $XV_{ij}(t)$ denotes the estimated value of the amount of sensed data transmitted to a neighbouring node at time $t$.

- **Transmission threshold** $T_\theta$: Every hop delay consists of the transmission delay over the wireless path and the queuing delay in the buffer of a receiver node. $T_\theta$ represents the amount of data queued at node $n_i$ [32].

- **Probability of a transmission failure** $Pr_i$: $Pr_i$ represents the probability of a transmission failure over the path $n_i \rightarrow n_j$ due to energy depletion, data hijacking, bad channel quality or collisions when sensor node $n_i$ transmits to sensor node $n_j$.

3.5 Data transmission

A source node that has data to transmit to the CH through the neighbouring nodes establishes a three-way handshake connection protocol to avoid data collision during transmission [33, 34]. First, it checks its tabu if paths to a CH do exist or not. If the paths exist, the source node transmits to a neighbouring node $n_i$ through an efficient path using Equation (4).
with each other through a wireless medium. These attributes left unattended for a long period. Sensor nodes communicate WSNs in most cases are deployed in the area of interest and

| TABLE 3 | PREQ format |
|----------|--------------|
| S_A_ID  | SN_ID | E'(n_i) | Hop Count | h(i) | Destination Address | Time-stamp t_s |

| TABLE 4 | PREP packet format |
|----------|-------------------|
| S_A_ID  | SN_ID | E'(n_i) | Hop Count | h(i) | Destination Address | Time-stamp t_{s_i} |


\[ S_A = \min \sum_{i=1}^{m} E'(n_i)d_{A,i} \]  

(4)

where \( S_A \) denotes source node, \( E'(n_i) \) is the current energy level of a neighbouring node, \( d_{A,i} \) is the distance between the \( S_A \) and \( n_i \). However, if the path does not exist, it broadcasts path request routing information (PREQ) to the neighbouring nodes to create paths to the CH. PREQ format is shown in Table 3.

where \( S_A \_ID \) denotes source node identification, \( SN \_ID \) denotes sensor node identification, hop count \( h(i) \) refers to the number of intermediate sensor nodes through which sensed data must pass between the SA and CH node. A neighbouring node that receives path request routing information (PREQ) updates its tabu with this routing information and subsequently forwards it to the next node, this process continues until it gets to the CH. Thus, each node in a cluster in which its path does exist sends path reply (PREP) back to the SA in the reverse way through which the PREQ was sent as shown in Table 4.

\( t_{s_i} \) is time taken for PREP to get to the \( S_A \). This process enables the \( S_A \) to construct multiple paths between the sensor nodes and transmits sensed data through an efficient path to the CH node using Equation (4). Step-by-step data transmission from source nodes to the CHs is presented in Algorithm 1.

Algorithm 1 Data Transmission from source nodes to CHs

Begin
1. Input \( S_A \), \( n_i \)'s, and \( CH_k \)
2. If a path exists between \( S_A \) and \( CH_k \) then
3. Transmit sensed data to \( n_i \) using Equation (2)
4. If data has not reached the \( CH_k \) then
5. \( n_i = n_i+1 \);
6. end if
7. else
8. Broadcast path request to all nodes in cluster \( k \) using PREQ and PREP formats
9. Go to step 2
10. end if
11. End

3.6 | Detection of malicious sensor nodes in WSNs

WSNs in most cases are deployed in the area of interest and left unattended for a long period. Sensor nodes communicate with each other through a wireless medium. These attributes make networks vulnerable to different attacks—the DoS attack in particular. In this work, the following methods are used to detect malicious nodes.

The proposed detection scheme sports a malicious node by comparing the energy dissipation of the nodes with the estimated energy. Normal nodes dissipate energy slowly during network operation. Conversely, malicious nodes use additional energy to launch DoS attacks in the network. A node can be identified as a malicious node if there is a significant difference between the energy consumption rate \( (E_p) \) and the threshold energy value \( E_θ \) of sensor nodes. Let \( E_R \) denote real energy consumption and \( E_X \) denote estimated energy values of sensor nodes. \( E_F \) is expressed as follows.

\[ E_F = \begin{cases} E_X & \text{if } E_R > E_θ \\ \end{cases} \]  

(5)

where \( E_θ \) is expressed as

\[ E_θ = \frac{m \bar{E_X}}{(m-1)\bar{E_R}} \]  

(6)

where \( m \) denotes the malicious node, \( \bar{E_X} \) denotes the average estimated energy value, and \( \bar{E_R} \) denotes the average real energy consumption. We believe that energy dissipation, \( E_F \), for all legitimate sensor nodes will approximately have the same values during a round time. However, if the value of \( E_F \) is greater than \( E_θ \) in a given period, then there is high probability that some nodes have been comprised and DoS attack is suspected in the network. In addition to confirm that a network is under attack, data packets’ transmission rate is further used to establish the presence of DoS attack in the network and it is presented as follows.

3.6.1 | Traffic intensity

The rate of the attack on traffic increases as the number of compromised nodes increases in the network, assuming that all such nodes are participating in the attack process. If the value of the traffic intensity of the sensor node is lower than or equal to the traffic threshold value during a round time, the node is considered as a legitimate node such that \( TR_{ij}(t) \leq EV_{ij}(t) \).

However, if the value of traffic intensity is greater than the traffic threshold value such that \( TR_{ij}(t) > EV_{ij}(t) \), then the nodes may have performed the attack as behaviour of DoS. The traffic intensity between two nodes is expressed as follows:
3.6.2 | Aggregator nodes vulnerability

In this subsection, we develop a model to show that aggregator nodes (CHs) are under DoS attack. We assume that CH nodes receive data packets from their member nodes and attackers are always target them. The average number of incoming traffic received by a CH $k$ at time $t$ be expressed as

$$\mathcal{B}_k(t) = (1 - \mu)\mathcal{B}_k(t - 1) + \mu \cdot \omega_k(t)$$

(8)

where $\mu$ ranging between 0 and 1 (i.e. $0 < \mu < 1$) is the weighted factor showing the vulnerability of the long-term average behaviour to the current bandwidth variation. The higher the value of $\mu$, the more dependence on the current variation. Deviation of incoming traffic from the average at time $t$ is expressed as follows:

$$D_{k, in}(t) = \max\{0, D_{k, in}(t - 1) + \omega_k(t) - \mathcal{B}_k(t)\}$$

(9)

During network operation, attackers launch DoS by constantly sending useless data to the CHs. The cumulative data transmission deviation would be noticeably higher than the expected data transmission. $TR_{ij}(t)$ and $D_{k, in}(t)$ are sensitive to the transmission rate and average incoming traffic respectively. The deviation from average $D^T$ is the sign of such an attack. $D^T$ is the incoming traffic received by CH $k$ at time $t$ and is expressed as follows:

$$D^T_{k, in}(t) = \frac{D_{k, in}(t)}{\mathcal{B}_k(t)}$$

(10)

Thus, if the $D^T_{k, in}$ is greater than a CH bandwidth threshold level $\Phi$, this increase in bandwidth is another signal that the network is under DoS attack. However, we expect $D^T_{k, in}$ to be much lower than $\Phi$ if there is no DoS attack.

3.7 | Lightweight evaluation in clusters

Complex methods may not be infeasible to evaluate sensor nodes due to their limited computation capacity and resource-constrained. We develop lightweight models to evaluate the trust values of sensor nodes. The CH $k$ in a cluster $C_k$ counts the successful delivery ratios of its legitimate sensor nodes. The current trust sensor nodes $n_i$ in the $C_k$ is defined as follows:

$$T(n_iC_k) = \frac{S(n_i)}{S(n_i) + F(n_i)}$$

(11)

where $T(n_iC_k)$ denotes the trust value factor of $n_i$, $S(n_i)$ and $F(n_i)$ denote the number of successful and unsuccessful data transmissions of $n_i$ per round respectively. The current trust values of cluster head $k$ $T(CH_k)$ are calculated in Equation (10):

$$T(CH_k) = \begin{cases} S(CH_k) \
\quad \quad \quad \frac{S(CH_k) + F(CH_k) + 1}{S(CH_k) + 1 + F(CH_k) + 1} \end{cases}$$

(12)

Thus, when the number of unsuccessful transmissions in the $CH_k$ increases, the expression $\frac{1}{F(CH_k)}$ decreases the trust value of $C_k$. Thus, Equation (12) soon decreases the trust value of the $CH_k$. A node $n_i$ is a malicious node for a $CH_k$ if it has transmitted to $CH_k$ at least once and $F(n_i) \geq S(n_i)$.

Therefore, a node in which the detection factor values of all its models developed above are more than the threshold values is termed a malicious node. Once the CHs detect that there are malicious nodes in the network and the communication channels are under DoS attacks, they forward the routing information of that node to the base station. The base station receives the information; it generates fresh IDs and sends them to all sensor nodes except all the malicious nodes. It deletes all communication paths of the malicious nodes from neighbouring nodes. If a sensor node does not have an ID, it cannot create any communication path. Therefore, other nodes will not be able to communicate with it. Similarly, the malicious nodes will not be able to communicate with other nodes, they become isolated. Detection of DoS attack workflow is presented in Figure 3.

3.8 | Trust computation in the data centre

Cluster head nodes intermittently forward the current trust aggregated data to the data centre. Thereafter, the data centre computes the aggregated trust value of sensor nodes $n_N$ as follows:

$$T(n_N) = \beta_1T_p(n_N) + \beta_2T_H(n_N)$$

(13)

It classifies the aggregated trust value into three groups as follows
Quality of service in wireless sensor networks

Since the existence of ubiquitous computing, sensor nodes are embedded in electronic devices. These wide range of applications have made WSNs an integral part of our lives [35]. Security issues must be resolved in order to fully exploit the potential applications of WSNs [36]. We further address security issues to include QoS in addition to security models we have developed to increase the security of applications in WSNs. The following factors: availability, reliability, and serviceability (ARS) are used to ensure that the integrity of data transmitted during network operation is maintained. QoS is a measurable level of service requirements to be met during data transmission from source nodes to a data centre. Conventional schemes of using sensor nodes and integrating ARS into WSNs to attain QoS can effectively improve not only the reliability of the overall networks but also the security challenges in WSNs [37]. Reliability of a network is the probability of its survival in a period. Due to resource-constrained and mode of data transmission of sensor nodes, individual nodes can fail or compromise. Thus, techniques to increase sensed data ARS during network utilization are necessary. We develop models for the three factors in order to maintain QoS under a range of network constraints. Average Time between Failure (ATF) and Average Time to Repair (ATR) are the terms used to express the factors for each sensor node. Average Time between Failure in a network with N sensor nodes is expressed as follows.

\[ \text{ATF} = \sum_{i=1}^{N} \frac{1}{\lambda_i} \]

It is assumed that the failure rate (\(\lambda\)) of each sensor node is the same.

### 3.9.1 Availability

Availability of each sensor node is measured as the probability that a network stays fully operational over a period of time. The availability of a sensor node is expressed as

\[ \text{Availability} = \frac{\text{Average Time between Failure (ATF)}}{\text{Average Time between Failure (ATF)} + \text{Average Time to Repair (ATR)}} \]

where \(f_1\) and \(f_2\) are used to vary the size of the three groups.

### 3.9.2 Reliability

Reliability is the ability of a network to successfully transmit sensed data from source nodes through the CHs to a data centre in a given period of time. It is expressed in terms of probability as follows.

\[ \text{Reliability} = 1 - \frac{t}{\text{ATF}} \]

where \(t\) denotes time in seconds of the network survivability.

### 3.9.3 Serviceability

Serviceability of a system is defined as the probability that a failed system will restore to the initial operation. It is closely related to the repair rate. It is expressed as follows.
\[ \text{Serviceability} = 1 - \exp \left( -\frac{t}{\text{ATR}} \right) \] (19)

The service requirements are expressed in some measurable metrics domains: additive, multiplicative and concave. Considering the representation for WSNs in Section 3.

Let \( \ell(n_1, n_2) \) denote the weight of each link with respect to metric \( \ell \) on route \( R \) from \( S_A \) to \( n_N \). Then, \( \ell \) is said to be additive metric.

**Additive:** \( \ell \) is additive; it is the sum of the delay of each hop,

\[ \ell(R) = \sum_{i=1}^{N} \ell(E_i), \text{ where } E \text{ is the number of links between the nodes, such that} \]

\[ = \ell(n_1, n_2) + \ell(n_2, n_3) + \ell(n_3, n_4) + \ldots + \ell(n_{N-1}, n_N) \]

**Multiplicative:** \( \ell \) is multiplicative; it is the product of every hop in the network,

\[ \ell(R) = \ell(n_1, n_2) \times \ell(n_2, n_3) \times \ell(n_3, n_4) \times \ldots \times \ell(n_{N-1}, n_N) \]

An example is reliability, the probability of a reliable link is in the range between 0 and 1 in which case \( 0 < \ell(n_i, n_{i+1}) < 1 \).

**Concave:** \( \ell \) is said to be a concave metric if \( \ell(R) = \min(\ell(E)) \) such that,

\[ = \min[\ell(n_1, n_2), \ell(n_2, n_3), \ell(n_3, n_4), \ldots, \ell(n_{N-1}, n_N)] \]

Example is bandwidth, for instance, the bandwidth of a route is determined by the link \( E \) with the minimum bandwidth.

### 3.10 Attack detection rates

The rate of traffic attack increases with the number of malicious nodes in the network, assuming that all such nodes are participating in the attack process. If the malicious nodes are deployed at different locations in the network as shown in Figure 2, more data packets will be generated from the distributed nodes. The network parameters that have a direct effect on the performance of the detection scheme are the initial energy of the sensor node and the number of nodes in the network.

The performance of various proposed schemes can be used to measure its accuracy and efficiency [38]. We further use the following metrics to determine the detection of DoS attacks accuracy for the proposed scheme. The false-positive (FP) rates and false-negative (FN) rates [36]. Each of the alarm rate is defined below:

**The false-positive (FP) rate:** The false-positive rate is defined as the fraction of the total number of legitimate nodes classified as malicious nodes, over the total number of sensor nodes.

\[ \text{FP} = \frac{\text{Data packets wrongly classified as malicious nodes}}{\text{Total number of sensor nodes}} \] (20)

**The false-negative (FN) rate:** The false-negative rate is defined as the fraction of the total number of malicious nodes classified as legitimate nodes, over the total number of sensor nodes.

**Detection rate (DR):** The detection rate is defined as the percentage of malicious nodes correctly classified as malicious nodes to the total number of malicious and legitimate nodes. It is determined using the expression below.

\[ \text{DR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \times 100\% \] (23)

**Detection time:** Detection time is the time it takes for a scheme to identify an attack during detection. A good detection method requires a low false alarm and a high detection rate.
Therefore, the effectiveness of the scheme can be determined by comparing the false alarm rate, detection rate, average data packet delay, and detection time.

4 | PERFORMANCE EVALUATION

We evaluate the performance of the attack detection scheme based on the total number of attacks successfully detected using the simulation parameters in Table 4 and different false alarms. We have conducted simulations with NS-2 to evaluate the performance of our proposed method and compared the performances with the related work. Simulation is performed over a network area of 100 m × 100 m with 100 randomly distributed sensor nodes. We generated random traffic to the CH to simulate DoS attacks. Thereafter, we run the algorithm which has been shown in Figure 4. Other simulation parameters are listed in Table 5. The following metrics are used to measure the performance of the proposed methods and presented as follows.

4.1 | Sensed data delivery ratio

Figure 3 shows the percentage of sensed data delivery ratio as the number of malicious nodes varied from one node to five nodes. The data delivery ratio decreases as the number of malicious nodes increases in the network. The reason is that data are dropped before the malicious nodes are identified and removed from the network. In addition, malicious nodes may receive data from legitimate nodes and refuse to transmit them further. Thus, as the number of malicious nodes increases, the total data delivery ratio decreases in the network.

4.2 | Delay

Delay is one of the metrics we used for analysing network performance. It is the difference in time when sensed data is transmitted from the sender node and when it is successfully delivered at the destination node. Figure 5 shows the effect of delay between two different networks. We looked at data
transmission delay in a normal network (no malicious node) and when there is/are attacker(s) (malicious nodes) in the network. In the absence of a malicious node, there is no delay in the network. Thus, as the number of attackers increases, the delay increases in the network as shown in the figure. This is due to the time the attackers used to intercept the message being transmitted, read the content, modify it, and send it to the destination node.

Tables 5 and 6 show simulation results of the detection delay for both linear traffic surge and sudden traffic surge scenarios of the DoS attack. The tables show the relationship of the false alarm rate and detection delay measured in terms of the number of the data packets received, number of the spoofed data packets in the network, and computing time. The traffic pattern changes for both scenarios after the start of the attack. The attacker’s traffic rapidly increased during a DoS attack.
4.3 | Detection rate

We investigated the detection rate of our approach and compared it with two related work to detect DoS attacks in the network as shown in Figure 6. The detection rate is the percentage of the number of DoS attackers detected to the number of attackers in the network. Our scheme is able to detect the malicious nodes present in the network as 100% while the detection rate in MADoS and FFUCA is 80.4% and 60.1%, respectively. The reason is based on the four stages of DoS attack detection we used for our approach. Thus, LSDoS performed better than the other two related schemes.

4.4 | Detection accuracy

We performed many rounds of simulation where a different number of normal nodes are deployed per round. We also varied the number of attackers against the number of nodes for each round of the experiment. We performed simulation on the developed algorithm by assigning two malicious nodes for every 10 normal nodes and continue progressively up to 100 nodes. Figure 7 shows the simulation result for DoS attack detection by varying the number of attacks from 2 to 20. Initially, the detection accuracy for the three algorithms is almost the same when the number of nodes is between 10 and 20 nodes. Thereafter, we could see that as the number of attackers increases the performance of the FFUCA and decreases MADoS, while the LSDoS maintains its consistency. It achieves 36.2% more detection accuracy compared to the two algorithms.

4.5 | Average data packet delay

Average end-to-end data packet delay against the number of sensor nodes was investigated and the result is presented in Figure 8. We observe that as the number of sensor nodes
increases, the number of sensor nodes vulnerable to DoS attacks likewise increases. This obviously affects data transmission and results in data packet loss in the network. Thus, average data packet’s delay in our scheme is least among the three schemes; hence it performs better than the other two related schemes.

4.6 | Energy consumption

Energy consumption is an important metric in WSNs which directly influences the network lifetime. Presence of malicious nodes in WSNs increase bandwidth and computational overhead with bogus data injected into the network. This depletes the battery resource of sensor nodes and causes energy drain. Figure 9 shows the energy consumption comparison between a normal network and network with malicious nodes. Thus, the more the number of malicious nodes in the network, the more energy is depleted.

In addition, the real energy consumption and the energy estimation of the malicious nodes are compared in Figure 10. Initially, the real energy consumption and the energy estimate result are the same. Thereafter, as the malicious nodes launch DoS attacks, they consume more energy due to the extra energy used to launch the attacks. Thus, the energy estimation result becomes different from the real energy consumption of the malicious nodes. The difference between energy estimation and real energy consumption leads to the detection of malicious nodes in the network.

4.7 | Throughputs of clusters

Throughput is defined as the total number of sensed data successfully delivered to the destination node over the simulation time. The higher the value of the throughput means the better performance of the scheme. Comparisons of throughputs of the clusters for three different conditions is shown in Figure 11. The throughputs of clusters without malicious nodes (our scheme) are much higher than that of clusters with malicious nodes (without security protection). Initially, throughputs of clusters with our scheme and without our scheme are close to each other; however, over time the throughputs in our scheme perform much better than the scheme without protection. In the clusters with malicious nodes, the throughputs considerably decrease by 12.9 kbps. Thus, after the malicious nodes are detected and their information is sent to the base station, the base station generates unique new IDs and sends them to all legitimate nodes. Therefore, malicious nodes cannot interact with other legitimate nodes in the network as discussed in Section 3. Hence, the throughputs of clusters in LShDoS may not be higher than that in the normal network.

The simulation result for the availability and reliability of sensor nodes to reveal QoS during network operation is presented in Figure 12. We observe that sensor nodes have more lifetime and they can reliably transmit their data to the data centre. The reason is that our approach is able to detect and remove all malicious nodes in the network. Thus, it extends the WSN’s lifetime utilization.

We investigate network throughput after the implementation of the models and the graph is presented in Figure 13. Sensor node availability is measured if it is able to transmit successfully to its corresponding CH within the allocated time. It takes a value of 0, if it cannot transmit within the allocated time or 1, if the node can transmit.

5 | CONCLUSION AND FUTURE WORK

In this article, we present an approach for detecting and removing DoS attacks in WSNs. The method of detection is based on using cluster heads which are monitoring the traffic intensity in clusters. A unique method is used for the selection of the cluster heads. We further developed algorithms and implemented them to detect malicious nodes in the network.
using a network simulator, ns-3. The results show that the proposed scheme can effectively detect and eliminate DoS attacks in WSNs. It gives significant results in terms of energy consumption, time detection, data reliability, throughput, and detection rate. It provides a better load of partition between node sensors. In the future, we wish to implement our scheme in a real testbed for this will help us to check if the scheme meets the resource constraints of WSNs.

ACKNOWLEDGEMENT

This work is supported by the Centre for Postgraduate Studies, Cape Peninsula University of Technology, Cape Town, South Africa.

REFERENCES

1. Akdike, M.M.: A summary survey on recent applications of wireless sensor networks. Proc. IEEE Stud. Conf. Res. Dev. 16-17, 485–490 (2013)
2. Bagula, A., Abidoye, A.P., Zodzi, G.-A.L.: Service-Aware clustering: an energy-efficient model for the Internet-of-Things. Sensors. 16(1), 1–9 (2015)
3. Dhuria, S., Sachdeva, M.: Detection and prevention of DDOS attacks in wireless sensor networks. In: Gregorio Martinez Perez, Krishin K. Mishra, Shailesh Tiwari, Munesh C. Trivedi (eds.) Networking Communication and Data Knowledge Engineering, pp. 3–13. Springer (2018)
4. Tunea, C., et al.: Ring routing: an energy-efficient routing protocol for wireless sensor networks with a mobile sink. IEEE Trans. Mobile Comput. 14(9), 1947–1960 (2015)
5. Naranjo, P.G.V., et al.: A prolong stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks. J Supercomput. 73(2), 733–755 (2017)
6. Darabkh, K.A. et al.: A balanced power-aware clustering and routing protocol for wireless sensor networks. Ad Hoc Netw. 82, 155–171 (2019)
7. Dutt, S., Agrawal, S., Vig, R.: Cluster-head restricted energy efficient protocol (CREEP) for routing in heterogeneous wireless sensor networks. Wireless Pers Commun. 100(4), 1477–1497 (2018)
8. Sah, D.K., Amgoth, T.: Parametric survey on cross-layer designs for wireless sensor networks. Comput. Sci. Rev. 27, 112–134 (2018)
9. Savaglio, C., et al.: Lightweight reinforcement learning for energy efficient communications in wireless sensor networks. IEEE Access. 7, 29355–29364 (2019)
10. Bhushan, B., Sahoo, G.: Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wirel. Pers. Commun. 98(2), 2037–2077 (2018)
11. Yuan, Y., et al.: Secure apit localization scheme against sybil attacks in distributed wireless sensor networks. IEEE Access. 6, 27629–27636 (2018)
12. Alzubaidi, W.K., Shaker, S.H.: Methods of secure routing protocol in wireless sensor networks. J. Al-Qadisiyah Comput. Sci. Math. 10(3), 38–55 (2018)
13. Rajendran, R., et al.: Detection of DoS attacks in cloud networks using intelligent rule based classification system. Cluster Comput. 22(1), 423–434 (2019)
14. Abidoye, A.P., Ochola, E.O.: Denial of service attacks in wireless sensor networks with proposed countermeasures. In: Shahram Latifi (ed.) Information Technology-New Generations, pp. 185–191. Springer (2018)
15. Yager, R.R., Espada, J.P.: New Advances in the Internet of Things, pp. 119–138. Springer (2018)
16. Li, J., et al.: A clustering based routing algorithm in IoT aware Wireless Mesh Networks. Sustain. Cities Soc. 40, 657–666 (2018)
17. Oreaveev, A., Akbas, S., Ozerdem, S.: Secure and reliable object tracking in wireless sensor networks. Comput Secur. 70, 307–318 (2017)
18. Mansouri, D., et al.: Preventing denial of service attacks in wireless sensor networks. Proc. Int. Conf. Commun. 8-12, 3014–3019 (2015)
19. Heinzelman, Chandrakasan, A., Balakrishnan, H.: An application - specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. 1(4), 660–670 (2002)
20. Fouchal, S., et al.: Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensor networks. Int. J. Commun. Syst. 28(2), 309–324 (2015)
21. Taylor, V.F., Fokum, D.T.: Securing wireless sensor networks from denial-of-service attacks using artificial intelligence and the clips expert system tool. In: Proc. International Conference on IEEE Southeastcon, Jacksonville, Florida, USA, April 4–7, pp. 1–6 (2013)
22. Zhang, H., et al.: Testing and defending methods against DoS attack in state estimation. Asian J. Control. 19(4), 1295–1305 (2017)
23. Osanaiye, O.A.A., Alfa, A.S., Haneke, G.P.: Denial of service defence for resource availability in sensor networks. IEEE Access. 6, 6975–7004 (2018)
24. Al-issa, A. L., et al.: Using machine learning to detect DoS attacks in wireless sensor networks. Proc. Int. Conf. Int. Joint Conf. Electr. Eng. Infor. Technol. 9–11, 107–112 (2019)
25. Younis, O., Fahmy, S., HEED: A hybrid, energy-efficient distributed clustering approach for ad-hoc sensor networks. IEEE Trans. Mobile Comput. 1(4), 366–379 (2004)
26. Kannan, G., Raja, T.S.R.: Energy efficient distributed cluster head scheduling scheme for two tiered wireless sensor network. Egypt. Infor. J. 16(2), 167–174 (2015)
27. Sundaram, S., Gharesifard, B.: Distributed optimization under adversarial nodes. IEEE Trans. Automat. Control. 64(5), 1063–1076 (2018)
28. Chauhan, R.: Review on security attacks and countermeasures in wireless sensor networks. Int. J. Adv. Res. Comput. Sci. 8(5), 128–139 (2017)
29. Arisi, M.H., et al.: Energy harvesting and battery power based routing in wireless sensor networks. Wirel. Netw. 23(1), 249–266 (2017).
30. Wang, J., et al.: An affinity propagation-based self-adaptive clustering method for wireless sensor networks. Sensors. 19(11), 2579 (2019)
31. Olusupo, T.O., Otero, C.E.: A framework for optimising the deployment of wireless sensor networks. IEEE Trans. Netw. Serv. Manag. 15(3), 1105–1118 (2018)
32. Liu, X., et al.: Taming uncertainties in real-time routing for wireless networked sensing and control. IEEE Trans. Smart Grid. 4(1), 288–301 (2013)
33. Abidoye, A.P., Obagbuwa, I.C.: Models for integrating wireless sensor networks into the Internet of Things. IET Wirel. Sens. Syst. 7(3), 65–72 (2017)
34. Heinzelman, W.R., Kulik, J., Balakrishnan, H.: Adaptive protocols for information dissemination in wireless sensor networks. Proc. Int. Conf. ACM MobiCom. 9924, 174–185 (1999)
35. Yahiaoui, S., et al.: An energy efficient and QoS aware routing protocol for wireless sensor and actuator networks. AEU Int. J. Electr. Commun. 83, 193–203 (2018)
36. Khan, T., et al.: A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. IEEE Access. 7, 58221–58240 (2019)
37. Sarkar, A., Murugan, T.S.: Cluster head selection for energy efficient and delay-less routing in wireless sensor network. Wirel. Netw. 25(1), 303–320 (2019)
38. Faheem, M., Gungor, V.C.: Energy efficient and QoS-aware routing protocol for wireless sensor network-based smart grid applications in the context of industry 4.0. Appl Soft Comput. 68, 910–922 (2018)

How to cite this article: Abidoye AP, Kabaso B. Lightweight models for detection of denial-of-service attack in wireless sensor networks. IET Netw. 2021;10:185–199. https://doi.org/10.1049/ntw.2.12011