# Evaluating DoS Jamming Attack on Reactive Routing Protocol in Wireless Sensor Networks

Opeyemi A. Osanaiye*, Ogundile O. Olayinka** and Folayo Aina ***

**Department of Computer Engineering, Nile University of Nigeria, Abuja, Nigeria*
***Department of Computer Science, Tai Solarin University, Ogun State, Nigeria*
**** School of Physiology and Computer Science, University of Central Lancashire, Preston, United Kingdom*

Corresponding email: opeyemi.osanaiye@nileuniversity.edu.ng

Wireless Sensor Networks (WSNs) over the years have emerged as the enabling underlining infrastructure for new wireless technology trends such as Internet-of Things (IoT) and Fog Computing. Its application spread across diverse fields such as agriculture, military, healthcare and home automation. Despite its promising attributes, it is characterized by its extremely limited resources such as battery energy and memory. Additionally, its deployment in hostile and unattended areas make it vulnerable to security attacks. One of such attacks is the denial of service (DoS) jamming attack that is perpetrated by malicious nodes emitting radio frequency signals to disrupt and interfere with the normal functions of the sensor nodes in the network. This eventually causes a denial of service in the network. Different routing protocols have been proposed over the years to guarantee reliable communication and maintain the network lifetime and functionality for a reasonable duration, notwithstanding DoS jamming attack. Therefore, in this work, we evaluate the effect of a constant jamming DoS attack on two key reactive routing protocols in WSN, ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR). Metrics such as packet sending ratio (PSR), packet loss (PL) and transmitted packets are used to measure the impact of constant jamming DoS attack in the network. Simulation results using network simulation 2 (NS2) and trace graph show that, irrespective of the adopted reactive routing protocol, the impact of the jamming attack is the same.

**Keywords**: AODV, DoS, DSR, Jamming attack, Routing Protocol, Wireless Sensor Networks.

## Introduction

Wireless sensor networks (WSNs) are sets of inexpensive low power sensor that transmit and receive information over a short distance through wireless medium. The sensor nodes in WSN exist without infrastructure and it is applied in divers' fields such as agriculture, emergency response unit, weather forecasting, battle filed intelligence surveillance and home automation (Ogundile and Alfa 2017). A typical deployment of WSN consist of tens to thousands of sensor nodes deployed to sense and transmit information from an area of interest, since deploying a single sensor node is limited in its function. The self-organising and self-healing feature of WSN has necessitated its deployment in

remote, unattended and hearse areas to transmit signals that can be accessed and interpreted by the end user.

WSN can be categorized according to its structure or deployed environment. The deployed nodes can either be of equal or varying capacity, depending on the architecture. The topological structure of WSN can be realistically grouped into two, namely, flat based (tree) and hierarchical based structures. In flat-based topology, all participating sensor nodes play the same roles in the network. On the other hand, in a typical WSN hierarchical topology, the sensor nodes are clustered into groups, where some nodes perform more functions in conveying the sense information to its destination (base station). In addition, the environment the sensor nodes are deployed can be grouped into five, namely, terrestrial WSN, underwater WSN, underground WSN, mobile WSN and multi-media WSN (Fouchal et al. 2015).

WSN in recent times have become the choice network solution for new wireless technologies such as Fog computing and Internet of Things (IoT); however, its open and shared nature, coupled with its resource constraint such as limited memory, battery energy, and bandwidth has made it vulnerable to both active and passive attacks (Osanaiye et al. 2019). One of such attacks is the DoS attack that aim to deplete and exhaust the limited resources in WSN to disrupt the existence and functionality of the sensor nodes and cause an outage. Jamming is a form of denial of service (DoS) attack where the attacker transmits high-range signals to disrupt normal communication using minimal power. This attack is often directed towards the communication channel of the sensor nodes to deplete its resources such as bandwidth, battery life and storage in order to prevent transmitted sensor signals from reaching its intended destination. Thus, it affects the reliability, functionality and availability of the network. Four common jamming attack strategy has been identified in the literature, these are constant jammer, random jammer, reactive and deceptive jammer (Osanaiye et al. 2018). These jammers use different techniques to cause a DoS attack. For example, reactive jammer continually senses the communication channel and only start transmitting when a legitimate signal has been sensed to cause collision. Constant jammer, on the other hand, do not follow any lay down protocol but continually transmit series of malicious electromagnetic wave or radio signals to interrupt legitimate signals in the communication channel (Osanaiye et al. 2018). This attack causes interference at the transmitting node to corrupt the received signals. When compared with reactive jammer, constant jammer requires high amount of power to constantly jam the communication channel, while the reactive jammer minimizes the rate of power consumed.

WSNs and ad-hoc networks have common features such as decentralized architecture and lack of infrastructure. Therefore, ad-hoc routing techniques have greatly inspired the development of WSN routing protocols, most especially in adopting multi-hop communication method to ensure reliable and efficient message transfer and maintain the network lifetime for a reasonable duration (Ogundile and Alfa 2017). Routing protocols in WSNs coordinate how sensor nodes communicate by ensuring that the most optimum path is transverse when information is being transmitted between nodes or from source node to the base station. This optimum path is dynamic; therefore, the routing protocol can change the network topology based on traffic balance, energy consumption, availability of radio links and quality of service (Del-Valle-Soto et al. 2015). In (Kumar et al. 2013), the existing routing protocols for WSNs are categorized into three major types: proactive, reactive and hybrid, while in (Erdene-Ochir et al. 2010), the routing protocols are grouped into four: probabilistic routing, flooding based routing, location based routing and hierarchical routing. Furthermore, the authors in (Ogundile and Alfa 2017) classified the existing routing protocols for WSNs into two major types: single-hop

communication and multi-hop communication methods.

Cases of jamming attacks have been reported in WSNs (Osanaiye et al. 2018), which has been catastrophic to both the sensor nodes and the functionality of the network. However, extensive evaluation has not been performed to assess the impact of jamming attacks on the routing protocol used in the network. Therefore, in this work, we assess and evaluate the impact of jamming attacks on the routing protocols used in WSNs. More specifically, our focus is to study and evaluate the impact of constant jamming DoS attack on reactive routing protocols (that is, ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR)). We evaluate the resilience of these two reactive routing protocols by monitoring the performance metrics, such as packet sending ratio (PSR), packet loss (PL) and transmitted packets. These metrics indicate the link state of the network and can provide an insight into how resilience the routing protocols are to jamming attacks for future improvement.

Closely related works have carried out analysis on the role of routing protocols on the resilience of WSNs during situation of jamming attacks. In (Del-Valle-Soto et al. 2015), the authors studied the behaviour of a recent routing protocol, multi-parent hierarchical protocol (MPH) with two other common protocols, AODV and DSR to reactive jamming attacks. A recent work in (Del-Valle-Soto et al. 2017) proposed a mitigation technique for jamming attacks by modifying the protocols they earlier studied to give MPH-M, AODV-M and DSR-M. The work in (Erdene-Ochir et al. 2010) studied the resilience of WSN routing protocols against selective forwarding attacks by compromised nodes.

In this work, we present a comprehensive evaluation of constant jamming DoS attack on two popular reactive routing protocols, AODV and DSR. We analyse the resilience of these routing protocols towards constant jamming attack by monitoring key performance metrics such as PSR, PL and transmitted packet. Results obtained using network simulation 2 (NS2) and trace graph show that, irrespective of the reactive routing protocol used, the impact of the constant jamming attack on AODV and DSR routing protocols is the same. Furthermore, this research has opened further research on the security consideration to enhance reactive routing protocols in WSNs. In this work, we have used ordinary sensor nodes and non-cluster head nodes interchangeably to mean the same.

The rest of the paper is organised as follows. The next Section presents related work followed by the Section that describes constant jamming DoS attack. We discuss different routing protocols in WSNs before presenting the simulation and experimental environment Section. The performance metrics and discussion of results were thereafter presented before the final Section that concludes the work.

**Related Works**

The widespread deployment of WSNs to enable recent state-of-the-art applications have made its security a current research trend. Its resource constraint has made it vulnerable to attacks such as jamming DoS attack that sends malicious signals towards legitimate sensor nodes and communication channels to consume resource and disrupt legitimate communication. Some previously proposed routing protocols were deployed without security consideration. Therefore, in this section, we review past works on the study of the resilience of routing protocols during denial of service attack in WSNs.

In El-Semary and Abdel-Azim 2013), a review of the different routing protocols in WSNs and their security issues are presented. Recently proposed secure routing protocols that considers energy efficiency and QoS were thereafter presented. In (Montez 2016), the authors studied jamming-aware routing in military WSN are studied and proposed an extension of destination sequenced distance vector (DSDV). The extended DSDV ensures that based on the knowledge of the geographical position of the

jammer and nodes, the route is kept far away from the jammer to ensure network stability for an extended period.

The work in (Zin et al. 2015) reviewed secured multipath routing protocols by analysing the security requirements and possible common attacks in WSN. The main priority of the deployed routing protocol is to ensure that the effect of intruders and routing attacks are limited by relying on the benefits proffered by multipath techniques to provide a secured data transmission in WSNs. The trio of tolerant-based, prevention-based and mixed-mode methods were proposed to achieve a secured multi-path routing in WSNs.

The resilience of three routing protocols, MPH, DSR and AODV to reactive jamming attacks in WSNs are studied in (Del-Valle-Soto et al. 2015). Results obtained from their simulation show that MPH, the more recent routing protocol, was able to tolerate jamming attacks to some extent as compared to DSR and AODV. This can be attributed to its ability to minimize and encapsulate network segments during an attack. Furthermore, the self-configuration attribute of MPH, which is derived from the combination of both proactive routes and reactive behaviour, gives it a better performance over both OADV and DSR. The authors in (Del-Valle-Soto et al. 2015) proposed a mitigation technique for reactive jamming attacks by modifying MPH, AODV and DSR to give MPH-M, AODV-M and DSR-M (Del-Valle-Soto et al. 2017). This modification ensures that whenever each node that houses the detection algorithm produce a positive result, the node is isolated, and the routing protocols adapt their paths to avoid these isolated nodes.

**Constant Jamming**

In a constant jamming attack, radio signals in form of random sequence of bits or electromagnetic waves, are continuously emitted into the communication channel, without following any protocol, in order to interfere with legitimately transmitted signals (Pelechrinis et al. 2011). These random bits are continually sent by the constant jammer to occupy the communication channel, thereby starving transmission initiated by legitimate nodes. Another consequence of constant jammer attack is the corrupt signal received by the receiving node due to collusion and interference. One of the major demerits of constant jamming attack to the attacker is that enormous energy is consumed, as a result of continuous emission of signals, which drains the battery life of the node. Therefore, to carry out a successful constant jamming attack, a regular supply of power is required.

**Routing Protocols in WSNs**

A vital part of the sensing system of WSN is the routing protocol that guarantees that data are reliably collected and disseminated. During the self-organizing process into tree structures, sensor nodes in WSNs rely on hard or soft routing state. Both routing states are used by sensor nodes in hierarchical routing to elect a leader (Manjeshwar, and Agrawal 2001). The mechanism of routing protocol can be majorly categorized into two, namely, neighbour discovery and flooding (Koliousis and Sventek 2007). The former is used to discover and maintain connectivity with its neighbours by exchanging messages periodically to ascertain the state of the nodes locally, within radio range. The latter, on the other hand, disseminates network state to distant nodes to maintain a global knowledge of the entire network. The sensor nodes use this local and global routing states to determine the best path for the signal to be transmitted.

Generally, in WSN, the bandwidth, memory and battery energy of the sensor nodes is very important and can be affected by the number of states maintained by the routing protocols. Therefore, the routing protocols can be improved if more state is maintained at the detriment of an increase utilization of the system resources (Koliousis and Sventek 2007).

Routing protocols in WSNs can be majorly classified into three, namely, proactive, reactive and hybrid (Del-Valle-Soto et al. 2015). Proactive routing protocol, which is often referred to as a table-driven routing protocol, involves each sensor node storing routing information of the network. This information is updated periodically or during a topological change in the network. Proactive routing protocol is characterized by its low latency which makes it suitable for real-time traffic. A major disadvantage of this protocol is the periodic updates that wastes the already constrained bandwidth of the network. Examples of proactive routing protocol are destination sequenced distance vector routing (DSDV) and optimized link state routing protocol (OLSR).

Reactive routing protocol, which is the focus of this work, is used to discover routes by flooding the Route REQuest (RREQ) packets throughout the network. Reactive routing protocol creates congestion during high activities, due to the busty nature of the generated traffic, which is caused by using the current status of the network. The delay experienced can be linked to route discovery process; however, during inactive periods, bandwidths and energy are saved.

Lastly, hybrid routing protocol combines the complementing features of both proactive and reactive routing protocol. One of such features is the low latency from the proactive routing protocol and the minimum bandwidth requirement of the reactive routing protocol. Hybrid routing protocol ensures a balance between both proactive and reactive routing protocols.

***Reactive Routing Protocol***

Reactive routing protocols were designed to reduce the cost of storage and bandwidth attributed to table driven protocols Niu et al. 2014). Reactive routing computes its route based on demand and are only established when it is required between the source and destination node. The established routes are created and maintained in two phases: route discovery and route maintenance. The route discovery occurs on-demand by flooding the RRQ packets throughout the network. As soon as a route is found, the destination responds with a RREP (RouteReply) which contains the route information transverse by the RREQ. In this work, we describe and analyse the impact of DoS jamming attack on AODV and DSR reactive routing protocols.

### A. *Ad Hoc On-Demand Distance Vector (AODV)*

AODV is a reactive routing protocol that reduces control traffic by establishing path requests on demand. It builds its routes by using a route request and route reply query circle between the source and destination node, without any prior information. The process of building the routes involve the broadcast of route request (RREQ) packets. When a node receives this broadcast, it checks its record to determine if the RREQ packet has been previously received. If the received packet is not registered, the receiving node retransmits it again, thereby increasing the hop count and creating a reverse path. Two cases have been established when a node that received RREQ packet can respond with RREP packet to confirm a route; the first is when the node is the destination and the second is when the node has an available path to the destination. This process continues until the source node is reached. In some instances, the destination node may receive RREP packets from different nodes, therefore suggesting that there are different possible routes to get to the destination (Del-Valle-Soto et al. 2015). In such instance, the source node has two criteria for selecting the best path: the route with the highest sequence number or the route with the least number of hops. When nodes have multiple possible routes to the same destination node, the nodes generally select the shortest route.

B. ***Dynamic Source Routing (DSR)***

DSR is a reactive routing protocol that provides an on-demand routing without tracking high-rate topology changes (Abushiba and Johnson 2015). DSR function by first checking its cache, when a source node has packets to transmit to a destination node, to determine if it has a route to that destination. If a route is available, a new packet header that contains the path to get to the destination is created. If no route is available in the cache, the node starts a discovery process by sending a RREQ broadcast packet containing both source node and destination node identifier whose route is to be discovered, with a unique identifier for the RREQ (Del-Valle-Soto et al. 2015). After receiving the RREQ, the node checks its cache to determine if it has a route to the destination node. If a route is obtained, the node responds with RREP to the source, as opposed to forwarding the RREQ. The RREP response contains all the nodes that the received RREQ has passed through. However, if the node does not find a route in its cache, it will input its address in the packet and forward it via a broadcast. As soon as the source node receives the RREP, it stores the route in its cache and add the route in the header of subsequent packets sent by the node. Some of the advantages of DSR protocol is its loop-free routing and fast route recovery when there is a route change in the network (Kumar et al. 2013).

**Simulation Environment and Experimental Set-up**

In this section, we describe our simulation scenario, topology and the tool used for this work. The network parameters and performance metrics are also highlighted to ascertain the resilience of reactive routing protocol to constant DoS jamming attack in WSNs.

Arranging sensor nodes into clusters have been widely deployed in WSNs to ensure that it efficiently sense and monitor the area where it is being deployed. The clustering deployment in WSNs reduce the energy consumed and ensures scalability, efficient data aggregation, fault tolerant, latency reduction and robustness (Su et al. 2005). A typical **clustered** WSN comprise of two sets of nodes; the ordinary member nodes known as the non-cluster head and the cluster head that coordinate member nodes attached to it. The ordinary sensor nodes sense information and forward to the cluster head. The cluster heads in turn retrieve messages from their respective members and transmit to the base station. The clustering topology is often regarded as a two-layer hierarchy WSN, where the cluster head is the upper layer and the ordinary sensor nodes operates in the lower layer.

Our simulation consists of static sensor nodes in a cluster-based topology. The sensor nodes consist of the ordinary sensor nodes (nodes 1,2,5,6,8,9,10), the cluster heads (nodes 3 and 7), and the attack nodes (nodes 0 and 4). The attack nodes send malicious signals, in form of constant jamming attack, majorly to the cluster heads and sometimes to the non-cluster head nodes to deplete its resources (See figure 1).

Figure 1. Cluster-based WSN

We have simulated the WSN sensor nodes with reactive routing protocols under a constant jamming attack using NS2 network simulator. NS2 is a discrete event simulator often used for simulating both wired and wireless network scenarios. The simulated network architecture consists of 11 nodes with an area of 812m x 612m. File Transfer Protocol (FTP) is used for generating traffic and runs on Transport Control Protocol (TCP). The values used in NS2 for our work is presented in the Table 1.

Table 1: Simulation parameters

| Parameters | Values |
|---|---|
| Channel type | Channel/wireless channel |
| Radio Propagation model | Propagation/TwoRayGround |
| Network interface type | Phy/WirelessPhy |
| MAC type | Mac/802_15_4 |
| Interface queue type | Queue/DropTail/PriQueue |

| | |
|---|---|
| Link layer type | LL |
| Antenna model | Antenna/OmniAntenna |
| Max packet in interface queue | 50 |
| Routing protocol | AODV/DSR |
| X dimension of topography | 812m |
| Y dimension of topography | 612m |
| Number of nodes | 11 |
| Time of simulation end | 10 |
| Traffic type | FTP |
| Packet size | 1500 Bytes |

As shown in Figure 1, nodes 0 and 4 are the malicious nodes that transmit the constant jamming signal, notwithstanding the state of the communication packets to cause collision and drop packets. These two malicious nodes often target the cluster heads (nodes 3 and 7) because they perform more functions, when compared to the non-cluster head nodes. Most WSNs are heterogeneous in reality; as such, the cluster head nodes have higher capacity with respect to sensing unit, processing subsystem, storage and power. Therefore, they are often targeted by the adversary, thus bringing down the entire sensor network. Outside the cluster heads, random malicious packets are also sent to the non-cluster head nodes to disrupt transmission.

**Performance Metrics and Discussion**

In determining the impact of jamming DoS attack on routing protocol in WSNs, performance metrics, such as packet delivery ratio (PDR) can be measured. PDR is the measure of the ratio of the number of transmitted packets that have been successfully delivered and acknowledged by the destination node to the number of packets sent by the source node. When a reliable transport protocol, such as TCP, is involved, the source node only confirms that the packets have been successfully delivered upon receiving an acknowledgement (ACK) packet from the receiving node.

$$\text{PDR}(\%) = \frac{number\ of\ packets\ received}{number\ of\ packet\ sent} \times 100$$

However, in this work, we measure the effect of jamming Dos attack on packet sending ratio (PSR), packet loss (PL) and transmitted packet (TP).

***Packet Sending Ratio (PSR)***: Determining the PSR of a network involves measuring the ratio of the number of packets sent to the number of packets intended to be sent by the source node during a given period. To obtain the number of packets intended to be sent by the source node, we first determine the time at which the channel is available to the node at that period and multiply it by the transmission rate. PSR is a good metric for determining the effect of jamming attack on the routing protocols of the transmitting node, using the carrier sensing as its medium access policy. Table 2 shows the PSR for the sensor nodes in our simulated constant jamming attack for both AODV and DSR.

Table 2. Jamming attack PSR values for sensor node

| Node | Generated Packets | | Sent Packets | | PSR | |
|---|---|---|---|---|---|---|
| | AODV | DSR | AODV | DSR | AODV | DSR |
| 0 | 617 | 617 | 617 | 617 | 1 | 1 |
| 1 | 24 | 24 | 24 | 24 | 1 | 1 |
| 2 | 85 | 85 | 85 | 85 | 1 | 1 |
| 3 | 1061 | 1061 | 1025 | 1025 | 0.96 | 0.96 |
| 4 | 529 | 529 | 529 | 529 | 1 | 1 |
| 5 | 144 | 144 | 144 | 144 | 1 | 1 |
| 6 | 59 | 59 | 59 | 59 | 1 | 1 |
| 7 | 1097 | 1097 | 684 | 684 | 0.62 | 0.62 |
| 8 | 129 | 129 | 129 | 129 | 1 | 1 |
| 9 | 415 | 415 | 415 | 415 | 1 | 1 |
| 10 | 453 | 453 | 453 | 453 | 1 | 1 |

From the table 2, it is observed that the PSR for the nodes are 1, with the exception of nodes 3 and 7. This is due to the fact that the nodes 3 and 7 are the cluster heads and are the main target of the attack nodes.

The cluster heads are often targeted by the adversary in a cluster-based topology scenario, as they perform tasks such as data aggregation for all nodes in the cluster before sending the data to be base station. This way, the cluster head serves as sink to other

member nodes and once it is brought down, the entire network is made unavailable.

These two nodes therefore show a decrease in PSR value, which is an indication of a jamming DoS attack.

Figure 2. Graph of PSR for constant jamming attack on sensor nodes

***Packet Loss***: Packet loss occur in WSN when packets from a transmitting node fail to reach the destination node. During jamming attack, the attack node transmits malicious packets towards the target node to disrupt legitimate transmission on the transmission channel, thus causing packet loss. To determine and analyse the lost packets, we use trace graph. Table 3 shows the packet loss from the sensor nodes in our simulated constant jamming attack.

Table 3. Packet loss values for nodes during jamming attack

| Node | Packets Loss | |
|---|---|---|
| | AODV | DSR |
| 0 | 8 | 8 |
| 1 | 3 | 3 |
| 2 | 4 | 4 |
| 3 | 27 | 27 |
| 4 | 4 | 4 |
| 5 | 6 | 6 |
| 6 | 3 | 3 |
| 7 | 27 | 27 |
| 8 | 14 | 14 |
| 9 | 14 | 14 |
| 10 | 6 | 6 |

Figure 3. Graph of packet loss for constant jamming attack on sensor nodes

From the graph presented in Figure 3, it is observed that the cluster heads, nodes 3 and 7, were the most affected by the jamming attack, as they are the key target nodes. Other non-cluster head nodes randomly targeted by the constant jamming attack also experienced some packet loss.

Enormous packet loss in WSN ensures communication does not take place and can be used to determine other closely related DDoS jamming attack metrics, such as, packet sending ratio (PSR) and packet delivery ratio (PDR). The transmitting node confirms that the packet was successfully delivered when it receives an acknowledgement packet from the destination node.

***Transmitted packet***: During a jamming attack, there is the possibility that a non-cluster head node in the network has been taken over or infiltrated by a malware and controlled remotely. In this situation, a prior knowledge of the average packet transmitted by each node in the WSN can be determined to get a pattern. A threshold can also be obtained to detect the presence of a malicious node that send packets profusely to jam the network and disable communication among nodes in the WSN. Table 4 presents the packets transmitted in a WSN by different nodes during a normal communication which is been jammed by two sensor nodes, nodes 0 and 4.

Table 4. Transmitted packet during constant jamming on sensor nodes.

| Node | Transmitted Packets | |
|---|---|---|
| | AODV | DSR |
| 0 | 617 | 617 |
| 1 | 24 | 24 |
| 2 | 85 | 85 |
| 3 | 1061 | 1061 |
| 4 | 529 | 529 |
| 5 | 144 | 144 |
| 6 | 59 | 59 |
| 7 | 1097 | 1097 |
| 8 | 129 | 129 |
| 9 | 415 | 415 |

| | | |
|---|---|---|
| 10 | 453 | 453 |

From the graph presented in the Figure 4 below, it is observed that nodes 3 and 7 generated enormous packets. This is because they are both cluster heads that serve as a gateway to other clusters. Furthermore, nodes 0 and 4 presents another high packet transmission as they are malicious nodes generating the jamming signals that depletes the resources of the sensor nodes and disrupt communication within the WSN. This metric can be used to detect the presence on an attack node in the WSN.

Figure 4. Graph of transmitted packet for constant jamming attack on sensor nodes

Other possible metrics that can determined include bad packet ratio (BPR), bit error rate (BER), energy consumption amount (ECA), signal-to-noise ratio (SNR) and Packet inter-arrival time (Osanaiye et al. 2018).

Analysing the results obtained show that surprisingly the different reactive routing protocols used (i.e., AODV and DSR) produced the same result throughout the entire experiment. This therefore means that none of the reactive routing protocol is more secured when it was first proposed.

WSNs are often deployed in remote, harsh and inaccessible environment and are often characterised by their resource constraints such as limited power, storage and bandwidth; therefore, securing the sensor nodes is very essential. Routing protocols for WSNs guarantee that data are reliably collected and transmitted and can be secured to be resilient to attacks such as jamming DoS attack.

## Conclusion

In this work, we evaluate the impact of jamming DoS attack on reactive routing protocol, AODV and DSR, in WSNs to determine their resilience. The work was simulated using NS2 and analysed using trace graph. Results obtained show that jamming DoS attack on WSNs had the same impact on both AODV and DSR reactive routing protocols using packet sending ratio, packet loss and transmitted packet. None of the reactive routing protocols under study had more resilience to jamming DoS attack, therefore further research can be done to enhance the security of these routing protocols to ensure resilience to malicious attacks such as jamming DoS attack.


## Acknowledgement

The authors are thankful to Nile University of Nigeria for their research support.


## References


Abushiba, W., & Johnson, P. (2015, September). Performance comparison of reactive routing protocols for Ad Hoc network. In *e-Technologies and Networks for Development (ICeND), 2015 Forth International Conference on* (pp. 1-5). IEEE.

Del-Valle-Soto, C., Mex-Perera, C., Monroy, R., & Nolazco-Flores, J. A. (2017). MPH-M, AODV-M and DSR-M Performance Evaluation under Jamming Attacks. *Sensors*, *17*(7), 1573.

Del-Valle-Soto, C., Mex-Perera, C., Monroy, R., & Nolazco-Flores, J. A. (2015). On the routing protocol influence on the resilience of wireless sensor networks to jamming attacks. *Sensors*, *15*(4), 7619-7649.

El-Semary, A. M., & Abdel-Azim, M. M. (2013). New trends in secure routing protocols for wireless sensor networks. International Journal of Distributed Sensor Networks, 9(5), 802526.

Erdene-Ochir, O., Minier, M., Valois, F., & Kountouris, A. (2010, April). Resiliency of wireless sensor networks: Definitions and analyses. In *Telecommunications (ICT), 2010 IEEE 17th International Conference on* (pp. 828-835). IEEE.

Fouchal, S., Mansouri, D., Mokdad, L., & Iouallalen, M. (2015). Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks. *International Journal of Communication Systems*, *28*(2), 309-324.

Koliousis, A., & Sventek, J. (2007). Proactive vs reactive routing for wireless sensor networks. *Department of Computing Science, University of Glasgow, Glasgow Google Scholar*.

Kumar, M., Gupta, I., Tiwari, S., & Tripathi, R. (2013, January). A comparative study of reactive routing protocols for industrial wireless sensor networks. In *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness* (pp. 248-260). Springer, Berlin, Heidelberg.

Manjeshwar, A., Agrawal, D.P.: TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. In:

Proc. of the International Parallel & Distributed Processing Symposium. (2001).
Montez, J. T. H. (2016). *Jamming-aware routing in military wireless sensor networks* (Doctoral dissertation).
Niu, J., Cheng, L., Gu, Y., Shu, L., & Das, S. K. (2014). R3E: Reliable reactive routing enhancement for wireless sensor networks. *IEEE Transactions on Industrial Informatics*, *10*(1), 784-794.
Ogundile, O.O. & Alfa, A.S. (2017). A survey on an energy-efficient and energy-balanced routing protocol for wireless sensor networks. *Sensor,* 17(1084), 1–51.
Osanaiye, O.A, Alfa, A. S., & Hancke, G. P. (2018). A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. *Sensors*, *18*(6), 1691.
Osanaiye, O.A, Alfa, A.S. and Hancke, G.P. "Denial of Service (DoS) Defence for Resource Availability in Wireless Sensor Networks", *IEEE Access*, 2018.
Osanaiye O.A, Ogundile O.O, Aina F.A & Periola A (2019). Feature Selection for Intrusion Detection System in a Cluster-based Heterogeneous Wireless Sensor Networks" - *Facta Universitatis, Series: Electronics and Energetics*, Vol.32 No. 2, June 2019, pp. 315 – 330
Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2011). Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications surveys & tutorials*, *13*(2), 245-257.
Su C.C., Chang K.M., Kuo Y.H., Horng M.F.: 'The new intrusion prevention and detection approaches for clustering-based sensor networks,' in IEEE Wireless Communications and Networking Conference, 2005, 4, pp. 1927-1932.
Zin, S. M., Anuar, N. B., Kiah, M. L. M., & Ahmedy, I. (2015). Survey of secure multipath routing protocols for WSNs. *Journal of Network and Computer Applications*, *55*, 123-153.

.