Volume: 12 Issue: 05 Pages: 4691-4696(2021) ISSN: 0975-0290

Detection of Jamming Attack using IEWMA in Clustered Wireless Sensor Network

S.G.Hymlin Rose
Assistant professor, Department of Electronics and Communication Engineering, St.Joseph College of Engineering, Chennai, Email:hymlinrose@gmail.com
Thilothi.R, Rubiya Banu.N,Sandhiya.A ,Sumithra.
Student, Department of Electronics and Communication Engineering, St.Joseph College of Engineering, Chennai

----------**ABSTRACT**----------
Wireless Sensor Networks (WSNs) in recent times, have become one of the most promising network solutions with a wide variety of applications in the areas of agriculture, environment, healthcare and the military. Notwithstanding these promising applications, sensor nodes in WSNs are vulnerable to different security attacks due to their deployment in hostile and unattended areas and their resource constraints. One of such attacks is the DoS jamming attack that interferes and disrupts the normal functions of sensor nodes in a WSN by emitting radio frequency signals to jam legitimate signals to cause a denial of service. In this work a step-wise approach using a statistical process controls technique to detect these attacks. We deploy an Improved Exponentially Weighted Moving Average (IEWMA) to detect anomalous changes in the intensity of a jamming attack event by using the packet Break Advent Time (BAT) feature of the received packets from the sensor nodes. Results obtained from a trace-driven simulation show that the proposed solution can efficiently and accurately detect jamming attacks in WSNs with little or no overhead.

Keywords - **Jamming; IEWMA; BAT, Energy: cluster**

Date of Submission: Apr 05, 2021 Date of Acceptance: Apr 23, 2021

1. INTRODUCTION

A typical WSN consists of hundreds to thousands of sensor nodes which can be categorized according to their structure (topology) and the environment in which they are deployed. Structurally, WSNs can be categorized according to the placement of the sensor nodes in the deployed environment. The three main types of WSN structure are flat-based (tree), cluster-based and hierarchical.

Jamming attacks is a form of DoS attack where an adversary transmits a high-range signal to disrupt communication. Generally, jamming can occur unintentionally in a wireless medium through situations such as noise, interference and collision, however, a jamming attack in a WSN is a deliberate attempt by an adversary to interfere with the physical transmission of signals during a communication process.

The main aim of a DoS attack is to direct malicious signals towards the sensor nodes

Communication channels to deplete their resources such as the battery life, bandwidth, and storage in order to prevent transmitted sensor data from reaching its destination, thereby affecting its long term availability.

A jamming attack in a WSN is catastrophic as it does not require any special hardware device or software to be perpetrated .It can be carried out by passively listening to the wireless medium in order to broadcast on the same frequency band as that of the legitimate transmitting signal. A typical jamming attack is characterized by high energy efficiency, low detection probability, and anti-jamming resistance .In WSNs, the physical layer and the MAC layer are the common targets of DoS jamming attacks[1].

In the physical layer jamming attack, an adversary with a high transmission power signal can jam the communication medium, as most WSN deployments operate on a single frequency. Most traditional defense techniques rely on using a spread spectrum to mitigate physical layer jamming attacks .This technique is resource intensive and does not directly fit in WSNs due to the energy constraints of the sensor nodes. The access layer jamming attack, on the other hand, is perpetrated by either corrupting the control packets or deliberately reserving the communication channel for a maximum allowable number of slots, to ensure other nodes experience a lower throughput as a result of not being able to access the communication channel.

Cases of jamming attacks at the network and transport layer have been reported, where malicious packets are injected on certain routes and SNY flooding attacks are directed towards the sensor nodes to consume their resources .Detecting jamming attacks in WSNs has been an ongoing research trend over the past decade as commonly proposed methods rely on dedicated devices or algorithms imbedded within the sensor nodes [2]. These methods often use information obtained a priori about the communication behavior during normal and jammed condition, which can be tracked using indicators and metrics obtained from different layers[3].

Example of these metrics is the received signal strength obtained at the physical layer and the packet delivery ratio at the application layer. Recently deployed methods have proposed a cross layer architecture to ease the collection of jamming attack indicators while other

Volume: 12 Issue: 05 Pages: 4691-4696(2021) ISSN: 0975-0290

proposed methods have combined two or more metrics to significantly improve the detection of jamming attacks .Closely related works have proposed packet Break Advent time as a metric in WSN to detect jamming attack situations.

2. RELATED WORK

Jamming in wireless mode of transmission disrupt environment in the form of noise, interference or collision. It over powers the transmitted signal by injecting high level of noise which lowers the signal to noise ratio, thereby reducing the probability of successful packet reception .hence it is so important than the other type attacks commonly available in the wireless sensor network [4].

A classification of the attack consists in distinguishing the passive attacks from the active attacks. The passive attack (eaves dropping) is limited to listening and analyzes exchanged traffic .this type of attack is easier realize, and it is difficult to detect .since the attacker does not make any modification on exchanged information. The intention of the attacker can be the knowledge of confidential information or the knowledge of the significant nodes in the network (cluster head node),by analyzing routing information, to prepare an active attack[5].

In the active attack, an attacker tries to remove or modify the messages transmitted on the network. It can also inject its own traffic or relay of old messages to disturb the operation of the network or the cause a denial of service [6]. Among the most known active attacks ,we can quote;

Tampering : it is the result of physical access to the node by an attacker ;the purpose will be to recover cryptographic material like the keys used for ciphering .

Black hole: a node falsifies routing information to force the passage of the data but itself ,later on ;its only mission is then ,nothing to transfer, creating a sink or black hole in the network.

Selecting forwarding: as mentioned above, a node play the role of router, in a selective forward attack, malicious node may refuse to forward certain messages and simply drop them.

Jamming: a well-known attack on wireless communication, it consist in disturbing the radio channel by sending useless information and the frequency band used these jamming can be temporary intermittent or permanent.

A technique to detect jamming is proposed and its is for cluster based wireless sensor network. The technique first divided the area where the network is formed into cluster head to be a legitimate node or a jamming node. Secondly, it declares the network as a node is exit in previous cluster .third, the behavior of the newly joined node in the cluster is monitored to be hammed or not and is keeps on tracking.

An approach has been developed to resolve the issue of DoS attack by implementing terminologies such as intruder detection system. It authenticate nodes with a key mechanism that is private key shared and retracing routing path as an repetitive action from the path involved with the affected node in the form of an attacker internal in the network. The primary focus of this proposed work is to contribute secure and reliable data transmission over source destination by resolving DoS attack. An intelligent hybrid WSN application that is using two approaches together with an aim to avoid DoS attack is presented. The main contribution of the work is to use a hybrid approach that handless the problem of jamming. The solution improves security by predicting against DoS and provides solution to the user by improving the PDR.

3. PROPOSED SYSTEM

The major goal is to secure the WSN against jamming attack .there are various type of defensive techniques in this area and several author proposed counter measure to defend jamming attack like hybrid approach frequency hopping spread spectrum and direct sequence spread spectrum. They provide resistance against jamming still they are not able to completely prevent the jamming and in some of the techniques if jamming is detected, the transmission stops. But rebroadcasting is needed to communicate as well as transfer the data. These inturn in need of new approach for jamming detection and preventing of data lose. Our proposed method overcome the above drawbacks and will achieve a high packet to delivery ratio.

3.1 JAMMING DETECTION METHODOLOGY

In this technique, the IEWMA algorithm is proposed, and it uses the packet BAT as the sole metric to distinguish between the normal traffic patterns and the jamming attacks. The IEWMA is a statistical monitoring technique that averages data and continually increases the weight of more recent values of the average variable. The packet BAT allows detecting different forms of Denial of Service (DoS) jamming attacks in WSNs.

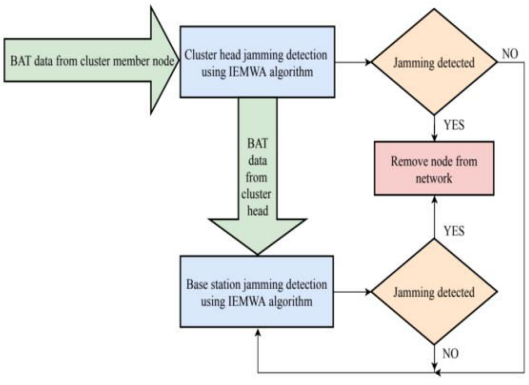

Fig 3.1 Representation of IEWMA algorithm

Fig 3.1depicts the jamming detection framework based on IEWMA. The CM senses information from the deployed area and process the information. It will send the processed information to the CH. The CH utilizes the jamming detection algorithm, IEWMA, by measuring the BAT of the packets received from the CM.

Volume: 12 Issue: 05 Pages: 4691-4696(2021) ISSN: 0975-0290

This identifies any discrepancy in the intensity of the received signal if a malicious node jams it. If there is a jamming attack in the network, the node which creates the jamming is first located based on the packet BAT, and then it is removed from the network.

If there is no jammed node present in the network, the BS receives the BAT data processed from the CH and check for any discrepancy in the signal. The BS calculates the BAT of the received packets to detect a jamming attack using IEWMA. If there is a discrepancy in the intensity of the received signal, then the node generating the attack will be traced and removed from the network.

Thus, both CM and CH nodes are checked for the presence of jamming node with the BAT and remove the node from the network if it is jammed. Therefore, this technique is highly advantageous in detecting the node, which creates jamming. Different steps include network initialization, energy-based clustering and route set-up using the OLSR algorithm, information transmission, and detection of the jamming node using IEWMA.

3.2 STEPS INVOLVED

- **Network initialization:** Nodes are deployed in this network.
- **Energy clustering**: After the node deployment cluster head and cluster member are identified based on energy.
- **Route setup using OLSR algorithm**: It's a proactive link state routing protocol, which used hello and topology control(TC)message to discover and then disseminate link state information throughout the network
- **Data transmission**: Data transmitted from one node to another node.
- **Detection of malicious nodes**: Once the data transmission process starts, the node will be checked for maliciousness in two places.
- **Jamming attack**: IEWMA algorithm is used for checking the jamming condition.

3.2.1 NETWORK SETUP

The network is the static structure that contains some of the data transmission functions. The Base Station (BS) transfers the network information to all the nodes. The network typically includes the pre-defined architecture like the sink node and the source node. To transmit data across the network, the origin node is created. This can be used by sender node for data communication. The other intermediate nodes are equipped with energy.

It is assumed that the nodes are randomly distributed in the field. After deployment, the nodes will neither be added nor deleted from the network. The assumption is that all the sensor nodes must have the same computing, communication, and storage capabilities. When the two nodes enter other communication ranges, each node in the network is essential to have some initial energy.

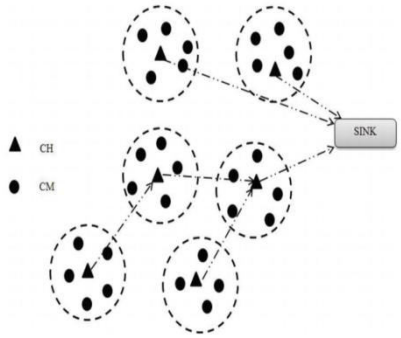

Fig 3.2 Network model

On this basis, the WSNs are abstracted by a graph $G= (N, E)$, in which N is the set of all nodes, and E is the set of all boundaries, *i.e.,* edges. The edge means that the two nodes are within the transmitting range of each other. Each node contains a list of its neighboring nodes, as shown in Fig 3.2.

If the sensor nodes in a WSN lack energy, they stop working, thus causing the entire sensor network to fail. Therefore, energy conservation is the main issue of WSN. Such protocols should be configured to use minimal energy for sensing, storage, and transmission.

To monitor and transmit data to the nearest node or Base Station (BS), some energy is consumed. The main requirement of the WSN is to reduce the consumption of energy and extend the lifetime of the network. When the sensor nodes in the network lose their battery power, communication between the sensor nodes stop.

To establish a secure link between the nodes, a proper data transmission routing technique should be adopted. An efficient routing method named as OLSR routing for the data transmission. This ensures that the mechanism for secure network information transmission is simple and efficient compared to the timestamp technique.

3.2.2 ENERGY BASED CLUSTERING

The next step is the clustering based on energy. The nodes are grouped into clusters using this mechanism. The clustering is merely grouping the nodes. The network nodes are organized into clusters. The successful clustering algorithm could do this. The clustering algorithm is used to group all the nodes within the network. The sensor node grouping is dependent on the energy in each sensor node. With some random energy, each sensor node is allocated, and the nearly equal energy nodes are formed as one unit and are called as a cluster.

The nodes with equal energy are formed as one group because the unbalanced clustering problem encountered in some of the techniques explained in the literature can be resolved. The cluster information will be updated to all the nodes once the network is organized. The structure of the cluster consists of two parts, named as the Cluster Head (CH) and the Cluster Member (CM). The node with the highest energy will be chosen as the CH, and the remaining nodes in the group are named as a CM, as shown in Figure 3.2.

Volume: 12 Issue: 05 Pages: 4691-4696(2021) ISSN: 0975-0290

The cluster function is valid when the cluster member truthfully transmits all the data to the nearest node. If there is a false node in the network, then the CH determines the member of the cluster that is incorrect. The clustering method is, therefore, a truthful mechanism for identifying the misbehaving network node. The main contributions of the Energy Efficient Cluster Head (EECH's) are given as follows:

1. Design a novel selection algorithm for Cluster Head (CH) in WSNs, which selects the CHs to create a linked network.

2. The residual energy of each sensor node is evaluated.

3.2.2.1 RESIDUAL ENERGY

The residual Energy (E_{res}) is called as the energy that remains in the node at the present moment of time. To make a node as a CH, it needs more residual energy than its neighboring nodes. Let E_i be the node's first energy, and the energy consumed by the node is given by the Equation after *t* time period.

$$E(t)=(n_{txp}\times \alpha)+(n_{rxp\times}\beta) \quad (3.1)$$

Where ,

n_{txp}= Number of data packets transmitted.

n_{rxp}= Number of data packets received.

α ,β= Constants in the range (0,1).

The *Eres* of a node at time *t* is computed using Equation

$$E_{res}=Ei-E(t) \quad (3.2)$$

3.2.3 ROUTE SETUP USING OPTIMIZED LINK STATE ROUTING

The route establishment can be done using many algorithms such as AODV,DSR,MPR,OLSR,etc. But OLSR can enhance the PDR and the quality of the network. Therefore OLSR is chosen in the proposed technique. The OLSR is a wireless routing protocol**.** The OLSR is a proactive routing link-state protocol that floods its neighbor's routing table with all the network nodes and then calculates the optimum routes locally. The OLSR is simple to implement and has less end-to-end average time. With rapid changes of origin and destination pairs, this protocol improves the suitability for the sensor network. The link for the control messages does not require this protocol to be reliable.

When using interfaces, the OLSR is simple, but the routing protocol can be integrated easily into existing operating systems without changing the Internet Protocol (IP) message header format. The protocol applies only to the routing table of the host . The OLSR can be subdivided into three major modules: neighbor/link sensing, multilink relaying, and link-state and route calculation.

3.2.4 JAMMING DETECTION USING IEWMA

The IEWMA can be used to detect small shifts in time series data. It is a statistically effective strategy. The IEWMA has advantages over other SPC techniques, such that it combines the historical and the current data to enable small changes to be detected quickly and easily in time series. The IEWMA operates only by setting the limits.

The threshold limits the standard performances before the regular updates of the observed data traffic are handled on the average .The IEWMA uses a constant for measuring the value of lambda. The weighting constant determines the value of the present as well as historical findings. The progressive process drift determines the sensitivity of the process, which is too small. The IEWMA can be computed using the following expression in equationn 3.3,

$$y(t)=\lambda.x(t)+(1-\lambda).y(t-1)$$
$$t=1,2,3,\ldots n \quad (3.3)$$

Where *y(t)* is the mean of historic data *x(t), t* is the observation time, *n* is the number of smoothing constant observations that are to be monitored, including *y(0)* and $0 < \lambda \leq 1$. The IEWMA depth is determined by the smoothing constant, λ. The large value of lambda is λ=1 which lends more importance to recent observations and therefore reduces the weight of the older observations and vice versa. The value of λ usually is less than 0.5. Nevertheless, the use of a very low value for λ can lead to insensitivity to moderate intensity and short duration attacks. Therefore, λ is chosen for 0.5 to 0.8 in training.

The estimated variance of the IEWMA statistic can be approximated using,

$$\sigma^2_y=\sigma^2_x(\lambda/2-\lambda) \quad (3.4)$$

Where,$\sigma_y$is the standard deviation obtained from the historical data. The control chart centerline is the target value. The Upper Control Limit (UCL) and Lower Control Limits (LCL) can be determined using the below Equations,

$$UCL_y=yo+f._y \quad (3.5)$$
$$LCL_y=y_o-f._y \quad (3.6)$$

Where f is the factor set to be equal to 3 sigma control limits.

The most exciting factor during the identification of the jamming assault is from the tops of the charts. There are occasions in which the traffic options discovered fall below or above the lesser control cap, which can be an anomaly of the network. The IEWMA jamming detection technique consists of 2 parts, the primary part being the training stage that involves capturing the traditional BAT from legitimate nodes in the cluster to obtain a traditional profile.

The second part is the IEWMA algorithm employed as a test part. If the jamming attack is detected, an alarm is activated, and the malicious node is disconnected from the network, as shown in Figure 3.1. If the maximum time of transmission is greater than the pre-selected duration (20 ms), then the data packet will be revealed as lost. The data packet will drop in the highly malicious node, and the majority of the lost packets will be triggered by malicious fall-off. It is advantageous over the timestamp technique with less routing overhead and energy.

4. SIMULATION RESULTS AND DISCUSSION

4.1 SIMULATION SETUP

In addition to the simulation parameters set out in Table 4.1, the performance of the IEWMA

Volume: 12 Issue: 05 Pages: 4691-4696(2021) ISSN: 0975-0290

technique shall be assessed using the Network Simulator 2 (NS2).

Table4.1 Simulation parameter configuration

Type of parameter	Value
Packet Size	64
Initial Time Value	0.05
BAT	38
No. of nodes	50
Simulation Area	500×500
Simulation Time	100 secs
Channel	Wireless
Propagation model	Two ray model
Communication Range	250m
Routing Protocol	OLSR

4.2 NODE DEPLOYMENT

In the network scenario, with random jamming nodes and the network traffic at varying data rates (200 kbps – 1000 kbps), the effectiveness of the IEWMA is evaluated. The network is designed with 50 nodes, with an origin node, a malicious node, a sink node, and other nodes with energy dependent clustering, as shown in Figure 4.1. The network area of 500 m × 500 m, with 50 sensor nodes is deployed. All the nodes have the same scope of communication range *R*= 250 m and the same capacity for processing.

When the network is formed, each node is built-in with its energy, and the nodes with the highest energy levels are grouped as CH. Besides, each node has its own routing table, nodal ID, cluster number, nearby nodes, and the number of hops to the neighbour node. Each node must give the nodal ID to all nodes on the network. The node '0' is to be chosen as the data centre (source node).

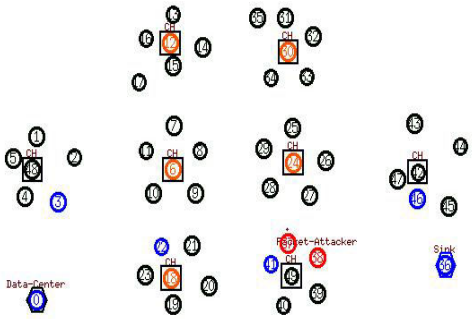

Fig 4.1: Clustering of nodes

The node 39 is the malicious node, which creates jamming. Node 0 is the source node and 36 is the sink node. The nodes 6,12,18,24,30,42,48 and 49 are the Cluster Heads (CH) selected based on the clustering algorithm.

4.3 TRANSMISSION OF NODE ID

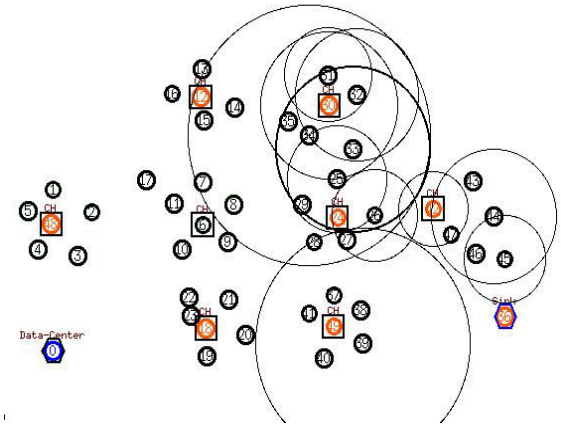

Fig 4.2: Transmission of Node information

Once the jamming node is identified, multiple routing tracks are chosen, if the nodes interact in the reliable range of coverage. A modified Dijkstra algorithm is used to determine the right path to transmit the data to the sink.

4.4 COPMUTATION OF IEWMA

The observed time series data depends on the values that appear prior or later in the series of data. In a practical case, it is examined with the time series data y(t), t=1,2,3…n.

Let us assume that

$$y(1)=0.9x(1)+0.1y(0)$$
$$y(2)=0.9x(2)+0.1y(1)$$
$$.$$
$$.$$
$$.$$
$$y(n)=0.9x(n)+0.1y(n-1)$$

The standard feature of the time series data increases with the rate; they are not mutually autocorrelated. Meanwhile, it indicates that there is no rapid change in the estimated values; a gradual increase may control the upper and lower control limits. After the intrusion of the jamming attack, the intensity of the value is reset in the other SPC techniques but in this approach, it is not necessary as the impact of the parameters is automatically adjusted between the upper and lower control limits.

4.5 PACKET DELIVERY RATIO:

Packet delivery ratio (PDR) can be measured as the ratio of number of packets delivered in total to the total number of packets sent from source node to destination node in the network. The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

Proportion of number of packets delivered against the number of packets sent. It can be calculated using the following function: Packet loss

Volume: 12 Issue: 05 Pages: 4691-4696(2021) ISSN: 0975-0290

ratio = (Ps − Pl) × 100 P s where is the number of packets sent, and is the number of packets lost during transmission.

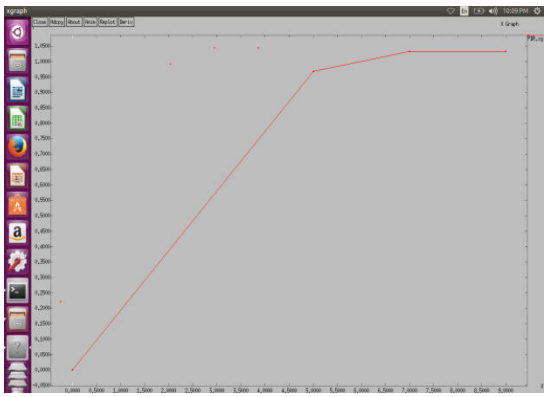

Fig:4.3 packet delivery ratio analysis.

4.6 THROUGHPUT ANALYSIS:

It is a measure of total unit of information a system can process in a given amount of time .Throughput is the actual amount of data that is successfully sent/received over the communication link .Throughput is presented as kbps, mbps or gbps and can differ from bandwidth due to a range of technical, including latency, packet loss, jitter and more.

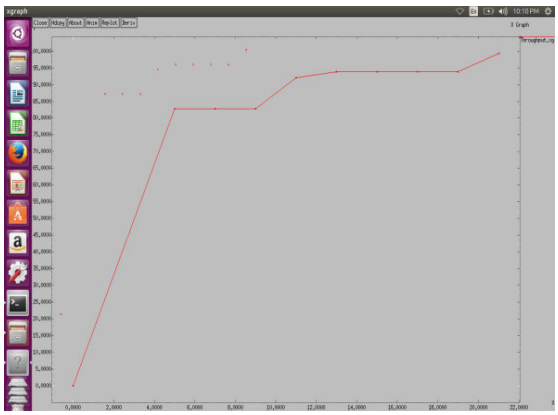

Fig 4.4 Throughput analysis.

Throughput generally gives the average at which over a communication network a data packet is delivered successfully from one node to another. It can be measured in bits per second .The calculation is **Throughput** = total good units produced / time.

5 CONCLUSION

It is a stepwise approach for detecting different forms of jamming attacks, where the jamming detector algorithm is deployed on the cluster head to detect attacks in the member nodes and also on the base stations to detect attacks in the cluster heads using the packet BAT metric. This metric is used to detect an abrupt change in packet sequence caused by a situation of jamming attacks using the IEWMA algorithm.

To demonstrate the efficiency of our proposed method, we conducted a trace-driven experiment using IEWMA to detect changes in traffic flow during situations of both non-jamming and jamming attacks. We evaluated our work using a non-jamming trace and the three different variations of jamming attacks from the dataset. Results obtained show that our proposed method can efficiently detect the presence of a jamming attack with little or no overhead in WSN. Our detection approach can be implemented on sensor nodes deployed in areas such as military battle fields, healthcare and mission-critical events, where sensed information needs to be transmitted in real time devoid of error. In the future, we plan to extend the evaluation of our proposed method using other datasets and deploy in real-world environment.

REFERENCES

1. Mingyan Li, Optimal jamming attack strategies and network defence policies in wireless sensor network ‘ ‘*IEEE transaction and mobile computing* (2010).

2. Sundaraguru, ‘Efficient Channel Access Model for Detecting Reactive Jamming for Underwater Wireless Sensor Network‘ *IEEE explore* (2020).

3. Manju .V, Sasikumar, Detection of Jamming Style DoS attack in Wireless Sensor Network‘ *IEEE International Conference on Parallel, Distributed and Grid Computing* (2012).

4. Osanaiye, O.A.; Alfa, A.S.; Hancke, G.P. Denial of Service Defence for Resource Availability in Wireless Sensor Networks, *IEEE Access* 2018, 6, 6975–7004.

5. Abduvaliyev, A.; Pathan, A.-S.K.; Zhou, J.; Roman, R.; Wong, W.-C. On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Common. Survey. Tutor*. 2013, 15, 1223–1237.

6. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Compute. Network*. 2008, 52, 2292–2330.

7.Li, M.; Koutsopoulos, I.; Poovendran, R. Optimal jamming attack strategies and network defencepolicies in wireless sensor networks. *IEEE Trans. Mob. Computer*. 2010, 9, 1119–1133.

8. Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *J. Network. Compute. Appl.* 2016, 67, 147–165.

9. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. *IEEE Common. Survey*. Tutor. 2011, 13, 245–257.