FBDR-Fuzzy Based DDoS Attack Detection and Recovery Mechanism for Wireless Sensor Networks

P. J. Beslin Pajila · E. Golden Julie · Y. Harold Robinson

Accepted: 16 August 2021 / Published online: 3 September 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
Wireless sensor networks (WSN) is considered as one of the exploring technology for its deployment of the massive number of dedicated sensor nodes which sense the environment and collect the data. The collected data are sent to the sink node through the intermediate nodes. Since the sensors node data are exposed to the internet, there is a possibility of vulnerability in the WSN. The common attack that affects most of the sensor nodes is the Distributed Denial of Services (DDoS) attack. This paper aims to identify the DDoS (Flooding) attack quickly and to recover the data of sensor nodes using the fuzzy logic mechanism. Fuzzy based DDoS attack Detection and Recovery mechanism (FBDR) uses type 1 fuzzy logic to detect the occurrence of DDoS attack in a node. Similarly fuzzy-type 2 is used for the recovery of data from the DDoS attack. Both the type 1 fuzzy-based rule and type 2 fuzzy-based rule perform well in terms of identifying the DDoS attack and recover the data under attack. It also helps to reduce the energy consumption of each node and improves the lifetime of the network. The proposed FBDR scheme is also compared with other related existing schemes. The proposed method saves energy usage by up to 20% compared with the related schemes. The experimental results represent that the FBDR method works better than other similar schemes.

Keywords Wireless sensor networks · Type 1 fuzzy logic · Type 2 fuzzy logic · Distributed Denial of Service (DDoS) attack · Network lifetime · Energy consumption

P. J. Beslin Pajila
beslin.kits@gmail.com

E. Golden Julie
goldenjuliephd@gmail.com

Y. Harold Robinson
yhrobinphd@gmail.com

1 Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

2 Department of Computer Science and Engineering, Regional Campus, Anna University, Tirunelveli, Tamil Nadu, India

3 School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India
1 Introduction

In recent times, Wireless Sensor Networks (WSN) has become one of the developing applications in the field of communication. It is a dynamic, quick to deploy and straightforward system. It is considered as an emerging technique because of the cheap price and productivity [1]. WSN has many sensor nodes, these sensor nodes are deployed in the environment to gather data and the gathered data can be sent to sink for further processing. The sink examines and integrates the data after receiving it from the sensor node. It has a connection to the outside world (end-user) through the internet [2]. With the support of Internet of Things (IoT) technology the sensor nodes collect the data, and the collected data can be forwarded through another sensor node till it reaches the sink [3]. The Nodes in WSN are usually deployed in static or dynamic framework with limited mobility and it is homogeneous or heterogeneous. However, the static sensor nodes are deployed in the fixed position, without mobility. Dynamic sensor nodes are mobility in nature, hence, the cost of the hardware is high and it utilizes more energy. The heterogeneous sensor nodes have different battery power for each node in the sensor network. But homogeneous sensor nodes have the same sensing range, same battery power, same communication range, same power in handling capability so it is very clear that homogeneous sensor nodes with mobility are the better option for real-time applications. WSN has wide-ranging applications for gathering data and data transmission in the military, health care, smart grid, surveillance, etc. They are exposed to security attacks due to security reasons. Hence, effective security measures are needed to secure the sensor nodes [4].

WSN is used to monitoring the communication between the sender and receiver that the communication is referred to as the transmission of sensed data. As the data never gets adulterated during the transmission it is difficult to detect the passive attack. The active attack is on the other hand usually modifies the data during its transmission between the sender and the receiver [5]. The DDoS attack, Node replication, Masquerade attack, Replay attack, Worm node, Sybil, Sinkhole, etc. are some of the active attacks. Among various active attacks, DDoS attack is one that affects the performance of WSN drastically, since it will flood the target node with a large number of packets so that the node will not be able to accept genuine requests [6]. The DDoS attack has more zombies so that it can create heavy traffic in the network. The zombie can also spoof the IP address and make it come under attacker control [7].

In a DDoS attack, the attacker uses multiple sources to transfer the malicious packets to the target node which results in more battery power usage of the target node. Further, as the user is flooded with more resources, it leads to less responsiveness and it consumes more energy [8]. The software used to perform DDoS attacks will have more basic logic structures and fewer memory sizes which aid the attackers to perform in an extremely easy way and to hide and enforce zombies. Moreover, DDoS attackers regularly change their methods to overcome security systems created by network managers and researchers who are already in constant alert to alter their methodologies in handling new attacks [9]. In a distributed environment, since the traffic is distributed, it is hard to differentiate normal packets with illegitimate packets which make it impossible to identify and stop this DDoS attack. The damage caused by a DDoS attack may lead to network or system shut down, rapid battery drainage of the sensor nodes and denial of services. Due to these issues, DDoS attack is considered as one of the serious attacks in WSN [10].
Fuzzy-based logic system is widely used to recognize the DDoS attack. This system is considered as the most effective attack detection method, which resolves with imprecise, vague boundaries among the normal traffic and various levels of attacks. It accurately detects the occurrence of the attack and it also identifies the strength of the attack [11]. Since early 1990’s fuzzy system has been implemented because of its adaptation capabilities. The growth has created a variety of fuzzy system that solves various types of problems in different application area [12]. There are various classifications in DDoS attack, among which flooding attack is considered in the proposed work. In this paper, the detection and recovery from DDoS (Flooding) attacks have been discussed.

The main contribution of the paper is.

- Type1 Fuzzy-based rule is framed to detect DDoS attacks with the input values of Energy Consumption, Response time and Packet count.
- The recovery model is constructed that the DDoS attacked node will be redirected to the sink using the alternate path.
- The identification of alternate path and the sink path are computed using the Type2 Fuzzy-based rule.

The rest of the paper is organized as follows. In Sect. 2, various fuzzy and machine learning techniques and comparative study between them is presented. Section 3, discusses the proposed fuzzy-based system. Section 4 contains the simulation results and performance evaluation and finally, Sect. 5 covers the conclusion respectively.

2 Related Works

The detection schemes for various DDoS attacks and detection of a DDoS attack in WSN is discussed in the literature survey. Xia et al. [11] proposed an intelligent fuzzy logic method that has two stages. The first stage is, the attack identification and the second stage is intelligent fuzzy logic, which was used for deciding the strength of DDoS flood attack. During the attack identification, for each new traffic, the co-efficient of the wavelet and SIC (Schwarz Information Criterion) statistic was updated. SIC is the technique used to evaluate repeatedly the network change-point. After identification, the network traffic is segmented into pieces and then the strength of the attack was identified based on fuzzy logic. The Hurst parameter also used to evaluate the strength of the DDoS flood attack. An intelligent DDoS judgement method [13] was proposed to detect the DDoS attack based on judgement. The Hurst parameter is calculated based on VTP (Variance-Time Plots), RVTP (Real-time Variance-Time Plots) and Real-time Detection of DDoS Attack based on Fuzzy Logic (FRVTP). The judgement is made by the result obtained from many DDoS attack. They analyzed the FRVTP method and traditional methods. From the comparative analysis made, it was found the FRVTP method given a better result in real-time. Fuzzy logic based defence mechanism [14] has four phases. They are the learning phase, Traffic analysis, Anomaly detection, and attack prevention. In the learning phase, the rules are created and framed inside the fuzzy system. This system learns the rule that was fed inside it. In the traffic analysis phase, the traffic is analyzed (normal or abnormal traffic) and evaluated based on the rules. In the anomaly detection phase, an alarm was generated if any malicious traffic found. The unwanted packets from the malicious node are discarded traffic in the attack prevention phase. Li et al. [15] proposed PCA-RNN (Principal Component
Analysis-Recurrent Neural Network) method to extract the features of the DDoS attack like flow time, slow connection, flood, etc. It is transformed into a PCA matrix for further analysis. PCA is the most efficient dimension reduction method. The correlated values are converted into values. The values are stored inside RNN to train it and the trained values are used to detect the DDoS attack. ML-based detection method [16] has two modules. The first module is pre-trained; it is already trained to find out the victim machine. The second module is online learning, it was trained by itself and updates the first module day-by-day. Four types of DDoS attack is detected using ML method and it prevents the attacks further affecting the system.

The Fuzzy logic methodology [17] uses the AODV protocol to evaluate different kinds of attacks. Among the attacks, the DDoS attack (Flooding) is identified, based on the transfer speed of data packets, loss of data packets and the delivery ratio. FBDPS(Fuzzy Based Detection and Prediction of DDoS Attacks) method [18], analyze the energy consumption of each node to predict the existence of the malicious node. According to this method, the nodes are compromised in the MAC layer by DDoS attack. The compromised nodes can be identified by the energy consumption rate. Usually, the malicious node while launching the attack, the energy consumption rate of a node varies. So based on that rate we can easily differentiate the normal node and malicious node. A threshold value is used for the energy consumption and packet delivery rate to classify a different kind of malicious nodes in the MAC layer. A fuzzy Markov chain model is used in FBDPS method to analyze the energy consumption of each sensor node. FLONF method [19] detect different kinds of DDoS attack like land attack, mail bomb attack, smurf attack and ping of death attack. Four different algorithms are used to detect such attacks. The detection is based on the flow rate and the number of flows. The algorithms used in this method detect the DDoS attacks faster and the rules for detecting the attack were also simple. FRI method [20] uses a fuzzy inference system for the detection of a DDoS attack. The fuzzy inference system stores the fuzzy input into the fuzzy set and calculates it. The calculated rules are used to detect the DDoS attack more efficiently.

The IPS based protection method [21] uses fuzzy logic and a Q-learning algorithm for detecting and preventing the system from the DDoS attack. It first analyzes the traffic in the network and then examines the DDoS attack utilizing a learning method and artificial intelligence. In this approach, the packets are captured and the details of the packets are collected. Then the collected details are stored inside the log files and the reliability index is calculated to identify the risk of the malicious packet. Now the abnormal behaviour of the node can be identified by using neuro-fuzzy rules. The Fuzzy Q-learning method is used for the quick detection of the DDoS attack. The Fuzzy Q-learning method will investigate each packet and checks for any abnormal behaviour in the packets. If any abnormal packets are identified, then those packets will be dropped. Then the result is stored to avoid the system from the same attack in the future. The fuzzy estimator method [22] is used to detect DDoS attack and to identify the IP address of the malicious one. It is identified to avoid further intrusion of DDoS attack. But the identified IP address is not so accurate. In the Bio-inspired Bat algorithm [23] is used to identify the attack as like the bat find its prey even in dark. It is an evolutionary-based algorithm, where each bat denotes a solution. It is the best method to detect the attack even in any situation but prevention is not possible. CNN Ensemble framework [24] encounters the most sophisticated DDoS attack in SDN and the detection is more accurate. Flexible SDN-based Architecture [25] detects and reduces the Low-Rate DDoS attack. It utilizes six Machine Learning models to train the SDN-based architecture to detect the attack more accurately. And the detection rate is up to 95%. MSCD method [26] has three parts to identify the clone attack. The first part
is to build the path of the head node and the second part is to decide the witness for each node in the network. Finally the third part is used to verify the legitimacy of the messages before sending to the head node in the witness ring. Novel intrusion detection technique [27] with PD (Pearson’s Divergence) is used to detect the intrusion that usually compromises the node. The compromised node exists for a long time in the network so that it can affect and collapse the system. Pearson’s Divergence technique is used to detect the attack and it improves the accuracy of the detection. SIP based defence mechanism [28] detects SR-DRDoS attack using IP spoofing technique. This type of attack improves the CPU load upto 100%. SIP mechanism has three modules named as statistics, Inspection and Action to identify the abnormal traffic to reduce the CPU load. The statistics module collects various traffics, Inspection module compares the traffic and finally action module identifies the abnormal traffic (SR-DRDoS attack) and drop or blocks it. IHSM Scheme [29] proposed three algorithms namely, EMABRD, SACOP and FZKA. EMABRD algorithm uses energy utilization threshold to identify the replica node. The detection rate of malicious node of SACOP algorithm is faster than EMABRD algorithm. FZKA algorithm stores the fingerprint of all the nodes in the cluster head and the fingerprint of the cluster heads will be stored in the base Station. So the cluster head and Base station involve in the detection of malicious node. FZKA algorithm also reduces the storage and communication overheads. OLWPRAD method [30] uses online dataset to detect the anomalies. It uses Principal Component Analysis (PCA) to manage the data. The detection of abnormal data in OLWPRAD can be done by dynamic threshold method. AIS-IDS method [31] is an effective approach to detect and reduce different kinds of flooding attack. It reduces the anomalies by dropping and blocking it. A distributed estimator framework [32] is used to detect randomly acquiring DoS attack or Data integrity attack. Each sensor is embedded with an statistical learning based detector and it is capable enough to detect the attacks effectively. SKG Scheme [33] identifies the active attacks while generating secret key. This scheme uses SVD technique and private pilot to identify the various active attacks. It usually authenticates the sender for protection against the active attacks. The DLDM Framework structure [34] is used to identify the different kinds of DDoS attack effectively, thereby it improves the throughput and it also reduces the energy consumption. EPSM [35] is proposed to detect the wormhole attack and it also used to minimize the energy consumption and the overhead of the network. The EPSM method has two stages to identify the wormhole attack. If both the stages are unsuccessful, it means that the attack is identified and the blacklist is announced. The MSIDN method [36] is used to identify and reduce the Distributed Denial of Service attacks and Flooding based DoS in Named Data Networking while Mitigation of the attacks will never damage the reliable users. It also reduces the traffic and network overhead. Lower-edge routers are used for stopping the malicious node from the origin. SDN-EHCND Mechanisms [37] is used to detect and keep away from the unnecessary nodes which occur because of cloning attack. The HCND method identify clone node and remove the clone attack available in the Wireless Networks. Superimposed SDIS junction code is used to find out the clones locally and globally. SLGBM method [38] is an intrusion detection method, it has two main algorithms they SLS algorithm and Light GBM algorithm. SLS algorithm minimize the communication overhead and the Light GBM algorithm detect the various network attacks in the WSN effectively. The summary of the related works is represented in Table 1.

EMA model [40] is used to detect the replica attack node based on the energy consumption of each node. This model has three phases, they are Energy Prediction, Threshold Setting and finally replica based detection process. In the energy prediction phase, energy of each node is identified by the amount of time the node exists in each state. And the
| Fuzzy method                                      | Parameter                                                      | Advantages                                                                 | Disadvantages                                                                 |
|--------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Intelligent fuzzy logic method [11]              | SIC statistics and Hurst Parameter                              | Detect DDoS attack very fast, successful and brilliantly                     | More time is utilized While calculating the change point of the network using SIC. Packet drop rate is high |
| An intelligent DDoS judgement method [13]       | Hurst Parameter                                                | Detect DDoS attack in real-time                                             | It lacks in self adaptability and the nodes consumes more energy              |
| Fuzzy logic based defence mechanism [14]        | Predefined learning rule(traffic parameters)                   | Predefined learning rule detects and mitigates DDoS attack very effectively | Difficult to get rid of sophisticated attacks and the nodes consumes more energy |
| PCA-RNN method [15]                             | Prediction Time and Performance metrics                        | Reduces the time of detection                                               | Less performance in the detection of the attack with real-time datasets and the packet drop rate is high |
| ML-based detection method [16]                  | Statistical features                                           | Detect DDoS attack with very low false positives and high accuracy          | The legitimate use of the machine is reduced                                  |
| Fuzzy logic methodology [17]                    | Trust value, Data Packet transfer rate, The delivery ratio of the data packet | Different types of attacks are detected by using a single method            | Data recovery and prevention method are not available and the data packet loss is high |
| FBDPS [18]                                      | Energy consumption rate                                        | Detection of the DDoS attack was made based on the energy consumption of the node | No prevention method and some nodes consume more energy so it is difficult to detect the attack more efficiently |
| FLONF [19]                                      | Flow rate, flow size in ICMP protocol is high                  | Very simple rules are used for detection                                  | No prevention method and the packet loss rate is high                          |
| FRI method [20]                                 | Packet size, packet count, Packet rate                         | Reduce false positive rate value                                            | No prevention Method and it reduce the network lifetime                       |
| IPS based Protection [21]                       | Fuzzy logic and Q-learning strategy                            | Security against Sophisticated attack, Less buffer size                    | Difficult to identify other attacks and it consumes more energy               |
| Fuzzy estimator method [22]                     | Packet arrival time                                            | Detect the DDoS before the resources consumed by the attack                | It is not so accurate in identifying the attacking IP address within the time limits and the response time is slightly high |
| Bio-inspired bat algorithm [23]                 | Classification of traffic                                     | Fast detection of DDoS attack                                               | No prevention method and the response time is high                             |
| CNN ensemble framework [24]                     | RNN,LSTM,CNN                                                   | Detection is more accurate                                                  | Prevention method is not available                                             |
| Fuzzy method | Parameter | Advantages | Disadvantages |
|-------------|-----------|------------|---------------|
| Flexible SDN-based architecture [25] | Random tree, random forest, support vector machine | Detection is accurate i.e., upto 95% and it also mitigate the LR-DDoS attack | Prevention method is not available |
| MSCD method [26] | Communication load | Probability of detecting the clone attack is more | Prevention is not available and nodes are not distributed uniformly in the network |
| Novel intrusion detection technique with PD (Pearson’s divergence) [27] | Probability and probability density function | It increases the detection accuracy | Prevention method is not available |
| SIP based defence mechanism [28] | Statistics, inspection and action | It detect the SR-DRDoS attack more quickly and thereby reduces the CPU load | Prevention method is not available |
| IHSM Scheme [29] | Energy consumption, fingerprint of nodes | FZKA algorithm performs better than the other algorithms and it improves the detection rate | Prevention method is not available |
| OLWPRAD method [30] | Principal component analysis | The detection rate is good compared to other machine learning algorithm | Prevention method is not available |
| AIS-IDS method [31] | Fuzzy logic | Detect and reduce the flooding attacks more effectively | Need to implement the method in real time environment and prevention method is not available |
| Distributed Estimator Framework [32] | False-data detector | Detect Dos attacks and linear attacks effectively | Difficult to detect complex coordinated attacks and prevention method is also not available |
| SKG Scheme [33] | SVD technique Private pilot | Identify different kinds of active attacks more effectively | Mitigation of the attack is not available |
| DLDM framework structure [34] | Deep learning techniques is used | Detect the DoS attack effectively and improves the throughput | Mitigation of the attack is not available |
| The EPSM method [35] | Secured AODV routing protocol algorithm is used | Detect the wormhole attack and also used to reduce the energy consumption | Mitigation and prevention method is not available |
| Fuzzy method                     | Parameter                                                                 | Advantages                                                                 | Disadvantages                                                                                      |
|---------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| The MSIDN method [36]           | Hop-by-hop signing and verification process. lower-edge routers            | Identify and reduce DDoS attacks and flooding based attacks very effectively | Prevention measures is not available. Collaborative actions like rate limiting and increased block periods should be included |
| SDN-EHCND mechanisms [37]       | Hybrid clone node detection mechanism Superimposed SDIS junction code and verification process | Detect the cloning attack more effectively                                | Attack mitigation is not available                                                                |
| SLGBM method [38]               | SLS algorithm Light GBM algorithm Machine learning algorithms             | Detect the various network attacks effectively. Accuracy rate is good. Calculation time is low and improves the overall performance | Running time is more and it does not mitigate the attacks effectively                                |
threshold is fixed in the threshold setting phase based on the prediction error, energy consumed in each state and the total number of messages sent and received by a node. In the final process, sink node will evaluate the actual energy consumption of each node. If the actual energy consumption of a node is more than the predicted energy consumption, then that node is considered as the malicious node.

DWA-SPS Mechanism [41] in the beginning generates all the paths from the source node to the destination node by using AOMDV (Adhoc On Demand Multipath Distance Vector) Protocol. After the generation of the multiple paths, source node will send the Detection Packet through the multiple paths to reach the destination node. Later the Feedback Packet produced from each intermediate node for the Detection Packet in the multiple paths. Then the comparison for the Feedback Packet with the Detection Packets was made by the source node. Based on the comparison the source node can able to detect the wormhole attacked path and it will send the packet to the secure optimal path, which was selected by using Particle Swarm Optimization Algorithm (PSO).

Mobile Malicious Node Detection Method [42] groups all the sensor nodes in different cluster. And the cluster head in each cluster uses rule-based anomaly detection method to identify the attack from the entire sensor node in the cluster. A mobile agent usually collects the data from all the cluster head and sends it to the sink. Before collecting the data from the cluster head, the mobile agent verifies whether the cluster head is trust worthy or not. Similarly the cluster head also checks whether the mobile agent is malicious or not. This verification process by the mobile agent and the cluster head can do by three-step negotiation process.

Neuro-fuzzy Based Intrusion Detection System [43], separates the suspected nodes from the normal nodes by using Fuzzy Inference rule. It uses the trust value to identify the malicious node. If the trust value of particular node is maximum, that node is considered as the legitimate node. If the trust value of a node is minimum or average, it is consider as the enemy node or distrust node. Finally the Artificial Neural Network is used to perform the refining process to identify the various DDoS attacks more accurately. The parameters like packet drop, residual energy, packet forward etc. of each enemy node and distrust node is given as the input to the ANN to identify the malicious node.

XGBoost classification model [44] mainly used for IDS dataset classification. This datasets are collected from the kaggle repository, where the data’s are in the form of categorical or numerical value. This data’s are converted into numerical value by one-hot encoding technique. Then the features of the dataset are standardized by using standard scalar technique. And the PCA algorithm is applied on the transformed dataset for dimensionality reduction and for more accuracy in detection of intrusion. Hybrid PCA-GWO method [45] was introduced to detect the intrusion in Internet of Medical Things. This method uses DNN model, which introduces PCA and GWA to analyze and predict the attacks very accurately. One-hot encoding is used to transform the collected data into numerical value and PCA-GWO is applied on to the transformed data to reduce the dimensionality. CANintelliIDS method [46] is the combination of both Convolutional Neural Network and Attention based Gatted Recurrent Unit (AGRU). It is mainly used to detect the single or mixed intrusion attacks in CAN bus. CNN gets the sequence of data from the various CAN bus to detect the pattern of anomaly. AGRU has reset and update gate to identify the amount of memory that is needed around it.

Based on the studies carried out in this field it is clear that the principal focus of most of the existing works are detecting the DDoS attack alone and there is no prevention measure available. Moreover the perfect level of reliability has not been accomplished due to their limited approach and concentration only on the application techniques. Therefore to deal with the problem a novel approach is proposed in this work.
3 Fuzzy Based DDoS Detection and Recovery Method

3.1 Proposed Work

Initially, nodes are deployed in the environment to form the network. The entire sensor nodes are randomly deployed with the same energy within the specified network area. Nodes can sense the environment in the form of data, these data packets are sent to the sink node. The packets are sent to the sink through the path which has been already calculated and identified; usually, the path is the collection of nodes. If any node in the path consumes more energy, and is flooded with data packets, it takes high response time and it is assumed that node is affected by DDoS (Flooding) attack. This prediction is made by type 1 fuzzy-based rule where energy consumption, response time and packet counts are given as the input parameters. If DDoS attack is detected, it is necessary to mark that particular node in that path as the dead node. To avoid the packet loss, the packet needs to be sent to the sink through the alternate path identifying the possible alternate paths to the sink. These paths can be identified based on a type2 fuzzy-based rule where distance, energy consumption, and packet size are given as the input parameters. From the thorough study that was made in fuzzy systems, it was very clear that the fuzzy system have a structure that is very simple and that can be established very easily too. Since the fuzzy system is more flexible, the rules can be changed at anytime. It is also deal with complex problems with indefinite inputs and makes decisions properly. It utilizes very less memory space.

3.2 System Mode

- The nodes are deployed randomly inside the network.
- Each sensor node is mobility in nature so that it can move inside the network area.
- Each sensor node is homogenous.
- A sink may be available anywhere inside the network area.

The nodes in the WSN are not protected against the DDoS attack. Usually, this attack drains the battery power of the sensor nodes and reduces its lifetime. To detect the DDoS attack and to secure the nodes from this attack, Fuzzy based DDoS detection and Recovery method has been proposed. It uses the type 1 fuzzy-based rule to detect the DDoS attack and type 2 Fuzzy based rule to secure the nodes. The workflow diagram for the proposed is shown in Fig. 1.

3.3 Detection Method

The Data Packets are sent from the source node to the sink. The sensor node transmits the data packets to the nearest node in the path to reach the sink. But, before passing the packets to a node, it is examined and evaluated based on the fuzzy logic. It has three input variables. They are Energy_consumption, Response_time, and Packet_count. Each and every node in the network have their own Energy Consumption, Response Time and packet count, which are stored in the routing table located in the sink. Based on the type1 fuzzy rule, the particular node was examined whether a DDoS attack occurs or not. Fuzzy logic
is used to determine the occurrence of DDoS attacks in a node based on a decision. It mainly uses true or false and “truth” degree.

The output is obtained based on the three inputs provided to the type1 fuzzy-based rule. The three inputs are considered as input parameters and each input parameter has membership functions. The membership function is mainly utilized for executing the element’s fuzziness in the fuzzy set. The fuzzy set is used for solving a problem depending on its experience. The output of type 1 fuzzy-based system depends on the input supplied to the fuzzy system.

The block diagram of Type1 Fuzzy based DDoS attack detection system is shown in Fig. 2, it has three input parameters they are Energy_consumption, Response_time, and Packet_count. The input parameters are supplied for the fuzzification process to obtain the fuzzy-based input value with the information provided by knowledge-based rule. Then the fuzzy-based value is sent for the defuzzification process and finally, the output is obtained by the defuzzification process. Based on the obtained output value we can verify whether there is a DDoS attack inside the network.
The type1 fuzzy-based detection system also has three inputs parameters and each parameter has three membership functions. Based on the input parameters and the membership functions 27 rules are formed. Table 2 represents the fuzzy rule for various inputs and outputs.

The algorithm1, which is mentioned below, represents the type 1 fuzzy-based DDoS attack detection algorithm. The current node collects the information (energy consumption, response time and packet count) from the next nearest hop to which it is about to send its packets and verifies the information using type 1 Fuzzy Based Detection method. If the energy consumed by the nearest sensor node is greater than the threshold energy value similarly if the response time and the packet count is more than the threshold value then that particular node is considered as malicious node. At once, the recovery method is called otherwise the normal broadcast takes place.

```
for(x1=currentnode; x1!=sink; x1++)
    for (y1=currentnode; y1!=sink; y1++)
        get nearest_hop(response_time,energy_consumption,packet_count);
        mem_func();
        fuz_rule();
    end for
end for
if (energy_consumption > Th_energy && response_time > Th_response_time && packet_count > Th_packet_count)
    node is declared as ddos attack
    recovery()
else
    normal broadcast
end if
```

Algorithm 1: Type1 Fuzzy based DDoS attack Detection algorithm
### 3.3.1 Input Membership Functions

The input and output member functions are framed by trapezoidal and triangular functions respectively. The Response_time membership function has variables like more, normal and less for evaluating the response time as shown in Fig. 3.

![Membership function of Response_time](image-url)
The response time has been measured by using the trained system as in FLQL method [21]. The Measurement of the membership function of Response_time for various variables like more, normal and less are represented in Eqs. 1, 2 and 3.

\[
\text{Response}_{\text{less}}(r) = \begin{cases} 
1, & r \leq 20 \\
\frac{40-r}{20}, & 20 < r
\end{cases}
\]

\[
\text{Response}_{\text{normal}}(r) = \begin{cases} 
\frac{r-40}{15}, & 40 < r \leq 55 \\
1, & 55 \leq r \leq 65 \\
\frac{80-r}{15}, & 65 < r \leq 80
\end{cases}
\]

\[
\text{Response}_{\text{more}}(r) = \begin{cases} 
\frac{r-80}{10}, & 80 < r < 90 \\
1, & 90 \leq r \leq 100
\end{cases}
\]

The Energy_consumption membership function has variables like high, medium and low for evaluating the energy consumption as shown in Fig. 4.

The Measurement of membership functions of Energy_consumption for various variables like high, medium and low are represented in Eqs. 4, 5 and 6.

\[
\text{energy}_{\text{low}}(r) = \begin{cases} 
1, & 0 \leq r \leq 10 \\
\frac{20-r}{10}, & 10 < r \leq 20
\end{cases}
\]

\[
\text{energy}_{\text{medium}}(r) = \begin{cases} 
\frac{r-20}{3}, & 20 < r < 23 \\
1, & 23 \leq r \leq 27 \\
\frac{30-r}{3}, & 27 < r \leq 30
\end{cases}
\]

\[
\text{energy}_{\text{high}}(r) = \begin{cases} 
\frac{r-30}{7}, & 30 < r < 40 \\
1, & 40 \leq r \leq 49
\end{cases}
\]

Similarly, the Packet_count membership function has variables like maximum, normal and minimum for evaluating the packet count as shown in Fig. 5.

The number of packets sent by a normal sensor node and malicious node varies, the packet count of each node can be measured accordingly [11]. The Measurement of the
membership function of Packet_count for various variables like maximum, normal and minimum are represented in Eqs. 7, 8 and 9.

\[
\text{Packet}_{\text{minimum}}(r) = \begin{cases} 
\frac{r}{15}, & 0 \leq r \leq 15 \\
1, & 15 \leq r \leq 25 \\
\frac{40-r}{15}, & 25 \leq r < 40 
\end{cases}
\]  

(7)

\[
\text{Packet}_{\text{normal}}(r) = \begin{cases} 
\frac{r-40}{10}, & 40 \leq r \leq 50 \\
1, & 50 \leq r \leq 60 \\
\frac{70-r}{10}, & 60 < r \leq 70 
\end{cases}
\]  

(8)

\[
\text{Packet}_{\text{maximum}}(r) = \begin{cases} 
\frac{r-70}{10}, & 70 \leq r < 80 \\
1, & 80 \leq r \leq 90 \\
\frac{100-r}{10}, & 90 < r \leq 100 
\end{cases}
\]  

(9)

Fuzzy rules are fixed for the constraints of the membership functions like Response_time, Energy_consumption and Packet_count are as shown in Fig. 6.

### 3.3.2 Output Membership Functions

MATLAB’s fuzzy rule viewer is shown in Fig. 7. IF–THEN conditions are used for generating fuzzy rules. The input and output of various membership functions are depicted in the fuzzy Table 2.

Membership functions for DDoS attack status:

\[
\text{DDoS attack}_{\text{status}}(r) = \begin{cases} 
\text{Occurred}, & r = 1 \\
\text{Prediction}, & r = 0.5 \\
\text{No_attack}, & r = 0
\end{cases}
\]  

(10)
3.4 Recovery Method

To recover the data packets from DDoS attack, in the proposed method, the packets which are sent to the node that is affected by the DDoS attack will be redirected to the sink through an alternate path. The nodes that utilizes less energy and which is very near to the sink are identified to redirect the data packets. To identify the alternate paths, a type2 fuzzy-based rule is used with the inputs parameters as Energy_consumption, Distance, and Packet_size. Once the alternate node is chosen, the node is examined again by the type1 fuzzy-based detection system to verify if the node is affected by DDoS attack or not. This process is called backtracking. The block diagram for the type2 fuzzy-based recovery system is represented in Fig. 8. The type 2 fuzzy based recovery system has three parameters (Distance, Energy_consumption and packet_size).

The fuzzy set has crisp input and it is given to the fuzzifier. The input (crisp) vector Inp’ = (Inp’₁,.....,Inp’ₚ) are represented as shown below [39].

\[
\sigma_{\text{Inp}_i}(\text{Inp}_i) = \begin{cases} 1, & \text{if } \text{Inp}_i = \text{Inp'}_i \\ 0, & \text{if } \text{Inp}_i \neq \text{Inp'}_i \end{cases}
\]

\[
\sigma_{\text{Inp}_i}(\text{Inp}_i) = \begin{cases} 1, & \text{if } \text{Inp}_i = \text{Inp'}_i \\ 0, & \text{if } \text{Inp}_i \neq \text{Inp'}_i \end{cases}
\]
The interval of the three inputs are $[0, 1]$. The inputs are Distance, Energy_consumption and the Packet_size. The rules for the fuzzy based recovery system are represented in the Table 3.

Based on the assumption the parameter for the input variables like Distance is considered as $i_p1$, Energy_consumption as $i_p2$, and finally Packet_size as $i_p3$. The variables for the outputs are Sink path identification as $GP1$ and Alternate path identification as $GP2$.
IF ip1 is FR1
  ip2 is FR2
  ip3 is FR3
      ........
  ipn is FRn
THEN
  jop1 is GP1
  jop2 is GP2

where $\sigma_{FRi}(inpi)$ is the lower membership function and $\sigma_{FRi'}(inpi)$ is the larger
membership function.

\[
fr(i) = \sigma FR1(\text{inp1}) \times \cdots \times \sigma FRp(\text{inpp})
\]  

(13)

\[
fr(i) = \sigma FR1'(\text{inp1}) \times \cdots \times \sigma FRp'(\text{inpp})
\]  

(14)

**Defuzzification**

\[
Dqi(y) = \frac{Dq1(y) + Dqjr(y)}{2}
\]  

(15)

The extended output,

\[
Dq_{cos} = [Dq1(y), Dqjr(y)]
\]  

(16)

Algorithm 2 represents the type2 fuzzy-based recovery algorithm, which is mainly used to redirect the packets to the sink through the alternate path. The current node collects the information from the next nearest hop to choose the correct path towards the sink. The path towards the sink can be identified based on decision made by type2 fuzzy based rule.

```
for(x=currentnode; x!=sink; x++)
    for(y= currentnode; y!= sink; y++)
        get nearest_nodej(distance,energy_consumption,packet_size);
        membership_fun();
        fuzzy_based_rule2();
    end for
end for
if (distance > Th_distance && energy_consumption > Th_energy && response_time > Th_response_time && packet_size > Th_packet_size)
    recover()
else
    normal broadcast
end if
```

Algorithm 2: Type2 Fuzzy based Recovery algorithm

The Distance membership function has variables like near, medium and far for evaluating the distance as shown in Fig. 9.

The Energy_consumption membership function has variables like less, medium and huge for evaluating the energy usages as shown in Fig. 10.

The Packet_size membership function has variables like small, medium and large for evaluating the size of the packets as shown in Fig. 11.

### 4 Performance Evaluation

In the proposed scheme FBDR method (Fuzzy Based Detection and Recovery method) is used to detect a DDoS attack. The sensor nodes are deployed randomly in a 500 × 500 m specified area. The sensor nodes are varied from 50 to 500. The sensor nodes are homogeneous so that all the nodes utilize the same energy, sensing range, etc. The sink is located
Fig. 9 Membership function for distance

Fig. 10 Membership function for Energy_consumption

Fig. 11 Membership function of Packet_size
anywhere in the specified area. The data packets from different sensor nodes are transferred
to the sink. Nodes are deployed only after the calculation of the Euclidean distance [3].

The Euclidean distance is calculated as

$$D(Se_i, t) = \sqrt{(q_i - q)^2 + (r_i - r)^2}$$  \hspace{1cm} (17)

The sensibility of $Se_i$ at the point ‘t’ can be represented as

$$Se_i(t) = \frac{Y}{D(Se_i, t)j}$$  \hspace{1cm} (18)

where $D(Se_i, t)$ be the distance between sensors. ‘$Se_i$’ be the sensors, ‘t’ be the point at posi-
tion $(q, r)$, $Y$, $j$ be the sensor dependent positive constant.

Euclidean distance is calculated to fix the distance between each sensor node. If the dis-
tance is less between the sensors, the sensitivity between the sensors is high so we need to
calculate Euclidean distance before deploying it in a position. The proposed FBDR method
reduces the usage of the buffer, energy consumption and response time. It also increases
the lifetime of the network and increases the live nodes even after 450 rounds. The pro-
posed method was evaluated and compared with the related DDoS detection strategies like
the FLQL method [21], FSDNA [25], SACOP algorithm [29] and DLDMFS[34] Table 4
represents the simulation parameters.

### 4.1 Network Lifetime

Figure 12 represents the lifetime of the network based on the different number of sensors.
It is mainly used to evaluate the capability of the FBDR method concerning the lifetime of
the network. The sensor nodes taken for our simulation work are 200, 300, 400 and 500. The fuzzy-based detection and recovery method is compared with the related strategies. As the count of the sensor nodes increases the lifetime of the network also gets increased. The FBDR method can save up to 30% of network lifetime compared to the other related strategies.

| Parameter                  | Value       |
|----------------------------|-------------|
| Network size               | $500 \times 500$ m |
| Nodes count                | 500         |
| ID of node                 | 16 bits     |
| Initial energy of node     | 1 J         |
| Data packet size           | 4000 bits   |
| Receiver transmitter expand| 1.1 dBi     |
| Sender transmitter expand  | 1.1 dBi     |
| Time taken for simulation  | 500 s       |
| Packets mean time          | 0.01 s      |
4.2 Number of Alive Nodes

Figure 13 represents the number of alive sensor nodes in each round. The FBDR method performs better than the other related strategies because there are alive nodes even after 450 rounds, but in the other related strategies, no more alive nodes available in 400 rounds which in turn affect the lifetime of the network. The distance between the sensors, while it is deploying in a position, has been evaluated by the Euclidean distance equation and it is found that the number of alive nodes is high in this method. Further, it is identified that all the sensors utilized very less energy if the distance between them is less and alive even after 450 rounds.
4.3 Packet Drop Rate

Figure 14 represents the FBDR method with less packet drop rate than the related strategies as FBDR method uses Fuzzy based type2 rule. It uses three types of inputs; they are Distance, Energy_consumption and Packet_size. These are used to analyze the DDoS attack affected nodes and the packets are redirected to the sink through an alternate path. It is found that, these inputs are not available in other strategies; the number of packets loss is higher in other related strategies.
4.4 Energy Consumption

Figure 15 represents the energy utilization of each sensor concerning the time. The FBDR method is compared with other related strategies. Since all the sensors are deployed very close to each other and the fuzzy-based rule is used, the sensor consumes very less energy than the sensors in the other related strategies.

4.5 Response Time

Figure 16 shows the response time concerning the time. The proposed FBDR method has 20% less response time than the other related strategies. Since the fuzzy-based rule is used for detection and fuzzy-based type2 rule is used for recovery. The response time of our proposed FBDR method has slight improvement over the other related strategies.

4.6 Buffer Usage

Figure 17 represents the utilization of buffer in the proposed FBDR method and other related strategies. The usage of the buffer is the main perspective for evaluating the overhead of the sensors. If the size of the buffer is less, the algorithm performs well. The FBDR method use 10% less buffer size than the other related strategies.

4.7 Detection Rate

Figure 18 represents the detection ratio in the proposed FBDR method and other related strategies. The detection rate of each strategy is evaluated and compared with each other. If the detection rate is more, the algorithm performs well. The detection rate of the proposed FBDR method is more than the other related strategies.
Fig. 17  Buffer usage in terms of time

Fig. 18  Detection rate in terms of the attackers count

Fig. 19  Execution time in terms of the node count
4.8 Execution Time

Figure 19 shows the execution time of the proposed FBDR method and the other related schemes with different number of sensor nodes. It is clearly visible that the FDBR method has less execution time compared to other related strategies. The proposed FDBR method has very less execution time and also very less computational complexity compared to other related strategies. The overall comparison of performance analysis is demonstrated in Table 5.

5 Conclusion

We propose a new FBDR method to detect the DDoS (Flooding) attack and to redirect the data packets to the sink through the alternate path. The FBDR method analyzes the energy consumption, response time and data packet count of each sensor. The FBDR method uses type1 fuzzy-based rule to detect the occurrence of the DDoS attack. So it quickly identifies the sensor node that was affected by the DDoS attack. Moreover, to avoid packet loss, the packets are redirected to the sink through the alternate path using the recovery method. The recovery method uses type2 fuzzy-based rule, by making an analysis on the packet size, energy consumption, and distance of each node. The proposed method saves energy usage by up to 20% compared with the related schemes. The proposed work examines the energy efficiency of the FBDR method by analyzing the buffer usage, packet drop rate, response time and a lifetime of the network. Based on the conclusion drawn from this study, the future focus would be the prevention measures using the neuro-fuzzy approach. From the conclusion made from this study, we aim to work on to enhance the FDBR method more up-to-date by combining both the benefits of neural network and Fuzzy Inference system. So that it can mitigate the DDoS attack in the early stage itself.
### Table 5  Detailed analysis

| Parameter considered                                    | Existing methods | Proposed method |
|---------------------------------------------------------|------------------|-----------------|
|                                                          | FLQL             | FSDNA           | SACOP Algorithm | DLDMFS | FBDR           |
| DDoS attack rate (in percentage)                        | 40               | 40              | 50              | 40     | 10             |
| Throughput (in percentage)                              | 60               | 50              | 50              | 40     | 80             |
| Communication OVERHEAD (in percentage)                  | 30               | 50              | 60              | 50     | 15             |
| Packet delivery ration (in percentage)                  | 90               | 85              | 80              | 80     | 98             |
| Power management                                        | Inadequate       | Unmanaged       | Inadequate      | Lowest | Fullest        |
| Mobility                                                | Limited          | Limited         | Limited         | Fixed base station | Fixed base station |
| Delay (s)                                                | 0.50             | 0.80            | 0.60            | 0.70   | 0.25           |
Author Contributions  P. J. Beslin Pajila: Writing—original draft, Writing—review & editing, Conceptualization, Data curation. E. Golden Julie: Data curation, Validation, Formal analysis, Supervision. Y. Harold Robinson: Conceptualization, Data curation.

Declarations

Conflict of interest  The authors declare that they do not have any conflict of interest.

Human and animal rights  This research does not involve any human or animal participation. All authors have checked and agreed the submission.

References

1. Patil, S., & Chaudhari, S. (2016). DoS attack prevention technique in wireless sensor networks. In 7th international conference on communication, computing and virtualization. Procedia Computer Science 79 (pp. 715–721). https://doi.org/10.1016/j.procs.2016.03.094.
2. Gavrić, Ž, & Simić, D. (2018). Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. Ingeniería e Investigación, 38(1), 130–138. https://doi.org/10.15446/ing.investig.v38n1.65453
3. Farsi, M., Elhosseini, M. A., Badawy, M., Arafat Ali, H., & Zain Eldin, H. (2019). Deployment techniques in wireless sensor networks, coverage and connectivity: A survey. IEEE Access, 7, 28940–28954. https://doi.org/10.1109/ACCESS.2019.292072
4. Kaur, A., & Kaur, M. (2016). Performance of node deployment techniques in WSN: A review. IJSRD - International Journal for Scientific Research & Development, 4(02), 2321–613.
5. Kaur, T., Saluja, K. K., & Sharma, A. K. (2016). DDoS attack in WSN: A survey. In International conference on recent advances and innovations in engineering (pp.1–5). https://doi.org/10.1109/ICRAIE39140.2016.

6. Shahzad, F., Pasha, M., & Ahmad, A. (2017). A survey of active attacks on wireless sensor networks and their counter measures. International Journal of Computer Science and Information Security, 14(12), 54–65.
7. Upadhyay, R., Bhatt, U. R., & Tripathi, H. (2016). DDOS attack aware DSR routing protocol in WSN. In International conference on information security & privacy (ICISP2015) (Vol.78, pp. 68–74). https://doi.org/10.1016/j.procs.2016.02.012.
8. Sachdeva, M., Singh, G., Kumar, K., & Singh, K. (2010). DDoS incidents and their impact: A review. The International Arab Journal of Information Technology, 7(1), 14–20.
9. Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defence mechanisms: classification and state-of-the-art. Computer Networks, 44, 643–666. https://doi.org/10.1016/j.comnet.2003.10.003
10. Mirkovic, J., Martin, J., & Reiher, P. (2003). A taxonomy of DDoS attacks and DDoS defense mechanisms. ACM SIGCOMM Computer Communications Review. https://doi.org/10.1145/997150.997156
11. Xia, Z., Lu, S., Li, J., & Tang, J. (2010). Enhancing DDoS flood attack detection via intelligent fuzzy logic. Informatica (Slovenia), 34, 497–507.
12. Alcala-Fdez, J., & Alonso, J. M. (2016). A survey of fuzzy systems software: Taxonomy. Current Research Trends and Prospects, IEEE Transactions on Fuzzy Systems, 24(1), 40–56. https://doi.org/10.1109/TFUZZ.2015.2426212
13. Jiangtao, W., & Geng, Y. (2008). An intelligent method for real-time detection of DDoS attack based on fuzzy logic. Journal of Electronics, 25, 511–518. https://doi.org/10.1007/s11767-007-0056-6
14. Iyengar, N. Ch. S. N., Banerjee, A., & Ganapathy, G. (2014). A fuzzy logic-based defense mechanism against distributed denial of service attack in cloud computing environment. International Journal of Communication Networks and Information Security (IJCNIS), 6, (3).
15. Li, Q., Meng, L., Zhang, Y., & Yan, J. (2019). DDoS attacks detection using machine learning algorithms, digital TV and multimedia communication. Communications in Computer and Information Science. Springer, Singapore, 1009 (pp. 205–216). https://doi.org/10.1007/978-981-13-8138-6_17.
16. He, Z., Zhang, T., Lee, R. B. (2017). Machine learning based DDoS attack detection from source side in cloud. In 2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud), New York, NY (pp. 114–120). https://doi.org/10.1109/CSCloud.2017.58.
17. Khare, A. K., Rana, J. L., & Jain, R. C. (2017). Detection of wormhole, blackhole and DDoS attack in MANET using trust estimation under fuzzy logic methodology. *International Journal of Computer Network and Information Security, 9*, 29–35. https://doi.org/10.5815/ijcnis.2017.07.04
18. Balarengadurai, C., & Saraswathi, S. (2013). Fuzzy based detection and prediction of DDoS attacks in IEEE 802.15.4 low rate wireless personal area network. *IJCSI International Journal of Computer Science Issues, 10*(6), 1. https://doi.org/10.1504/IJTMI.2013.056424
19. Tabatabaei, S. F., Salleh, M., Abbasy, M. R., & Torkaman, M. R. N. (2011). Denial of service (DoS) attack detection by using fuzzy logic over network flows. In *The 2011 international conference on security & management*.
20. Almseidin, M., & Kovacs, S. (2018). Intrusion detection mechanism using fuzzy rule interpolation. *Journal of Theoretical and Applied Information Technology, 96*(16).
21. Sherazia, H. H. R., Iqbalb, R., Ahmadc, F., Khand, Z. A., & Chaudary, M. H. (2019). DDoS attack detection: A key enabler for sustainable communication on the internet of vehicles. *Sustainable Computing: Informatics and Systems, 23*, 13–20. https://doi.org/10.1016/j.suscom.2019.05.002
22. Shiaeles, S. N., Katos, V., Karakos, A. S., & Papadopoulos, B. K. (2012). Real-time DDoS detection using fuzzy estimators. *Computers & Security, 31*, 782–790. https://doi.org/10.1016/j.cose.2012.06.002
23. Indraneel, S., & Vuppala, V. (2017). HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. *Applied Computing and Informatics, 15*, 59–66. https://doi.org/10.1016/j.aci.2017.10.003
24. Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Raymond Choo, K. K., & Iqbal, J. (2020). A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. *IEEE Access, 8*, 53972–53983. https://doi.org/10.1109/ACCESS.2020.2976908
25. Pérez-Díaz, J. A., Valdovinos, I. A., Choo, K.-K.R., & Zhu, D. (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access, 8*, 155859–155872. https://doi.org/10.1109/ACCESS.2020.3019330
26. Tang, C., & Han, D. (2020). A low resource consumption clone detection method for multi-base station wireless sensor networks. *IEEE Access, 8*, 128349–128361. https://doi.org/10.1109/ACCESS.2020.3007388
27. Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Raymond Choo, K. K., & Iqbal, J. (2020). A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. *IEEE Access, 8*, 53972–53983. https://doi.org/10.1109/ACCESS.2020.2976908
28. Pérez-Díaz, J. A., Valdovinos, I. A., Choo, K.-K.R., & Zhu, D. (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access, 8*, 155859–155872. https://doi.org/10.1109/ACCESS.2020.3019330
29. Tang, C., & Han, D. (2020). A low resource consumption clone detection method for multi-base station wireless sensor networks. *IEEE Access, 8*, 128349–128361. https://doi.org/10.1109/ACCESS.2020.3007388
30. Gavel, S., Raghuvanshi, A. S., & Tiwari, S. (2020). A novel density estimation based intrusion detection technique with Pearson’s divergence for Wireless Sensor Networks. *ISA Transactions*. https://doi.org/10.1016/j.isatra.2020.11.016
31. Poornima, I. G. A., & Paramasivan, B. (2020). Anomaly detection in wireless sensor network using machine learning algorithm. *Computer Communications, 151*, 331–337. https://doi.org/10.1016/j.comcom.2020.01.005
32. Scaranzi, G. F., Carvalho, L. F., Barbón, S., & Proença, M. L. (2020). Artificial immune systems and fuzzy logic to detect flooding attacks in software-defined networks. *IEEE Access, 8*, 100172–100184. https://doi.org/10.1109/ACCESS.2020.2997939
33. Huang, Yu., Jin, L., Zhong, Z., Lou, Y., & Zhang, S. (2019). Detection and defense of complex attacks on distributed state estimation. *Information Sciences, 547*, 539–552. https://doi.org/10.1016/j.ins.2020.08.008
34. Aliady, W. A., & Al-Ahmadi, S. A. (2019). Energy preserving secure measure against wormhole attack in wireless sensor networks. *IEEE Access, 7*, 84132–84141. https://doi.org/10.1109/ACCESS.2019.2924283
35. Premkumar, M., & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocessors and Microsystems, 79*, 103278. https://doi.org/10.1016/j.micpro.2020.103278
36. Benmoussa, A., el Karim Tahari, A., Kerrache, C. A., Lagraa, N., Lakas, A., Hussain, R., & Ahmad, F. (2020). MSIDN: Mitigation of sophisticated interest flooding-based DDoS attacks in named data networking. *Future Generation Computer Systems, 107*, 293–306. https://doi.org/10.1016/j.future.2020.01.043
37. Devi, P. P., & Jaison, B. (2020). Protection on wireless sensor network from clone attack using the SDN-enabled hybrid clone node detection mechanisms. *Computer Communications, 152*, 316–322. https://doi.org/10.1016/j.comcom.2020.01.064

38. Jiang, S., Zhao, J., & Xu, X. (2020). SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments. *IEEE Access, 8*, 169548–169558. https://doi.org/10.1109/ACCESS.2020.3024219

39. Balaji, S., Julie, G., Rajaram, M., & Robinson, H. (2016). Fuzzy based particle swarm optimization routing technique for load balancing in wireless sensor networks. *World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering, 10*, 1384–1393.

40. Anitha, S., Jayanthi, P., & Thangarajan, R. (2020). Detection of replica node attack based on exponential moving average model in wireless sensor networks. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07648-w

41. Tamilarasi, N., & Santhi, S. (2020). Detection of wormhole attack and secure path selection in wireless sensor network. *Wireless Personal Communications, 114*(1), 329–345.

42. Gandhimathi, L., & Murugabooopathi, G. (2021). Mobile malicious node detection using mobile agent in cluster-based wireless sensor networks. *Wireless Personal Communications, 117*(2), 1–14. https://doi.org/10.1007/s11277-020-07918-7

43. Sinha, S., & Paul, A. (2020). Neuro-fuzzy based intrusion detection system for wireless sensor network. *Wireless Personal Communications, 114*(1), 835–851. https://doi.org/10.1007/s11277-020-07395-y

44. Bhattacharya, S., Maddikunta, P. K., Kaluri, R., Singh, S., Gadekallu, T. R., Alazab, M., & Tariq, U. (2020). A novel PCA-firefly based XGBoost classification model for intruder detection in networks using GPU. *Electronics, 9*, 219. https://doi.org/10.3390/electronics9020219

45. Swarna Priya, R. M., Maddikunta, P. K., Parimala, M., Koppu, S., Gadekallu, T. R., Chowdhary, C. L., & Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Computer Communications, 160*, 139–149.

46. Rehman, A., Rehman, S. U., Khan, M., Alazab, M., & Reddy, T. (2021). CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU. *IEEE Transactions on Network Science and Engineering*. https://doi.org/10.1109/TNSE.2021.3059881

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

P. J. Beslin Pajila is currently working as an Assistant Professor, Dept of CSE in Francis Xavier Engineering College, Tirunelveli. She has published several papers in International Journals. She has presented many papers in National and International conferences in IoT, Mobile Computing and Network Security. Her area of interest is IoT, Machine Learning, Wireless Sensor Networks, Soft Computing and blockchain. She has the Total Teaching Experience of 9 Years.
E. Golden Julie is currently working as a Senior Assistant Professor in the department of computer science and Engineering, Anna University, Regional Campus, Tirunelveli. She has received Ph.D. degree in Information and Communication Engineering from Anna University, Chennai in the year 2017. Completed M.E. degree in Computer Science and Engineering in Nandha Engineering College, Tamilnadu in the year 2008 and did her B.E. Computer Science and Engineering in Tamilnadu College of Engineering, Coimbatore Tamilnadu. She is having more than 12 years of experience in teaching. She has published more than 34 papers in various International Journals and presented more than 20 papers in both national and International Conferences. She has written 6 book chapters by Springer, IGI global Publication. She is acting as an editor for a book title as “Successful Implementation and Deployment of IoT Projects in Smart Cities”, IGI Global in The Advances in Environmental Engineering and Green Technologies (AE EG T) book series. She is one of the editors for the book “Handbook of Research on Blockchain Technology: Trend and Technologies” published by Elsevier. She is acting as a Reviewer of many journals like computers and electrical Engineering Elsevier publisher & got the best reviewer certificate, Wireless Personal Communication by Springer Publication. She has given many Guest Lecturer in various subjects such as multicore Architecture, operating system, compiler design in Premier Institutions. She has acted as a jury in National level and international IEEE Conferences, project fair and Symposium. She has attended various Seminars Workshops and Faculty Development Programmes to enhance the knowledge of the student’s community. Her research area includes Wireless Sensor Adhoc Networks, Soft computing, blockchain, IoT and Image Processing. She has published research papers in various SCI journals like wireless personal communication, IEEE access, Ad-hoc networks, Mobile network and application, Journal of Ambient Intelligence and Humanized Computing, Peer-to-Peer Networking and Applications, Journal of Intelligent & Fuzzy Systems, Computer Standards & Interfaces and Earth Science Informatics. She is an active lifetime member in Indian Society of Technical Education.

Y. Harold Robinson is currently working in the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore. He has received Ph.D. degree in Information and Communication Engineering from Anna University, Chennai in the year 2016. He is having more than 15 years of experience in teaching. He has published more than 50 papers in various International Journals and presented more than 45 papers in both national and International Conferences. He has written 4 book chapters by Springer, IGI global Publication. He is acting as an editor for a book Title as “Successful Implementation and Deployment of IoT Projects in Smart Cities”. IGI Global in the Advances in Environmental Engineering and Green Technologies (AE EG T) book series. He is one of the editor for the book “Handbook of Research on Blockchain Technology: Trend and Technologies” publish by Elsevier. He is acting as a Reviewer of many journals like Multimedia Tools and Applications, Wireless Personal Communication by Springer Publication. He has given many Guest Lecturer in various subjects such as pointer, operating system, compiler design in Premier Institutions. He has also given an invited talk in technical symposium He has acted as a Convener, coordinator and jury in National level and international IEEE Conferences, project fair and Symposium. He has attended various Seminars Workshops, and Faculty Development Programmes to enhance the knowledge of student’s community. His research area includes Wireless Sensor Networks, Ad-hoc Networks ,Soft computing, blockchain, IoT and Image Processing. He has published research papers in various SCIE journals like wireless personal communication, IEEE access, Ad-hoc networks, Mobile networks and application, Journal of Ambient Intelligence and Humanized Computing, Peer-to-Peer Networking and Applications, Journal of Intelligent & Fuzzy Systems, Computer Standards & Interfaces and Earth Science Informatics. He is also an active life time member in Indian Society of Technical Education.