IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 October 2023, accepted 22 October 2023, date of publication 25 October 2023, date of current version 1 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3327516

RESEARCH ARTICLE

Analysis and Attack Detection in GSM Mobile Network With an Intelligent Jammer Using ANFIS Classifier

S. SIVAPRAKASH[1], (Member, IEEE), U. V. ANBAZHAGU[2], IYAPPAN PERUMAL[1], V. VINOTH KUMAR[3], (Member, IEEE), T. R. MAHESH[4], (Senior Member, IEEE), AND SURESH GULUWADI[5], (Member, IEEE)

[1]School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology University, Vellore, Tamil Nadu 632014, India
[2]School of Computing, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Chennai 600001, India
[3]School of Computer Science Engineering and Information Systems (SCORE), Vellore Institute of Technology University, Vellore, Tamil Nadu 632014, India
[4]Department of Computer Science and Engineering, JAIN (Deemed-to-be University), Bengaluru 562112, India
[5]Department of Mechanical Engineering, Adama Science and Technology University, Adama 302120, Ethiopia

Corresponding author: Suresh Guluwadi (suresh.guluwadi@astu.edu.et)

ABSTRACT A Mobile Ad hoc Network (MANET) is an autonomous system comprising mobile nodes that self-organize and connect via wireless networks, without reliance on a predefined infrastructure. These nodes are inherently susceptible to jamming, a form of denial-of-service attack that renders mobile services unavailable in the affected area. In this work, we introduce an intelligent jammer, constructed based on the Received Signal Strength Index-based Transmission Power Control (RSSITPC) Algorithm. This algorithm leverages Received Signal-Strength Indicator (RSSI) data to ascertain the optimal transmission powers for neighboring nodes and dynamically adjust these powers. The design of the intelligent jammer system incorporates a circuit interface, power unit, power detector, and GSM scanner. It employs a DAC-centered RSSITPC Algorithm to differentiate the jamming signal from legitimate signals by comparing the voltage in the received signal. Following the design phase, a Jamming Attack (JA) analysis is conducted, utilizing metrics such as the Packet Send Ratio (PSR) and Packet Delivery Ratio (PDR). Subsequently, a Hybrid Cross-layer Rate Adaptation (CLRA) Scheme is implemented to enhance JA detection and improve Wireless Link Utilization. The Adaptive Neuro-Fuzzy Interference System (ANFIS) classifier is then used to categorize data as either attack or regular data. For regular data, the Control Channel Attack Prevention (CCAP) algorithm is applied as a preventive measure. The proposed system's effectiveness is validated through comparative performance analysis with other widely used systems. Additionally, considerations are made for the adaptability of these methodologies to evolving intrusion techniques and changing network environments, as well as their scalability in larger, more complex networks.

INDEX TERMS Adaptive neuro-fuzzy interference system, control channel attack prevention algorithm, hybrid cross-layer rate adaptation scheme, intelligent jammer, received signal strength index-based transmission power control algorithm, received signal strength indicator.

I. INTRODUCTION

Wireless systems, due to their inherent openness, are prone to various malicious attacks. These vulnerabilities can be classified into three categories: i) eavesdropping attacks, where an adversary snoops on the wireless channel to extract information, ii) Jamming Attacks (JA), where the jammer transmits data or energy to disrupt reliable data reception or transmission, and iii) hybrid attacks, where the adversary can either actively jam or passively eavesdrop on any ongoing transmission [1]. Given the openness of wireless communications, attackers can eavesdrop on communications,

The associate editor coordinating the review of this manuscript and approving it for publication was Jad Nasreddine.

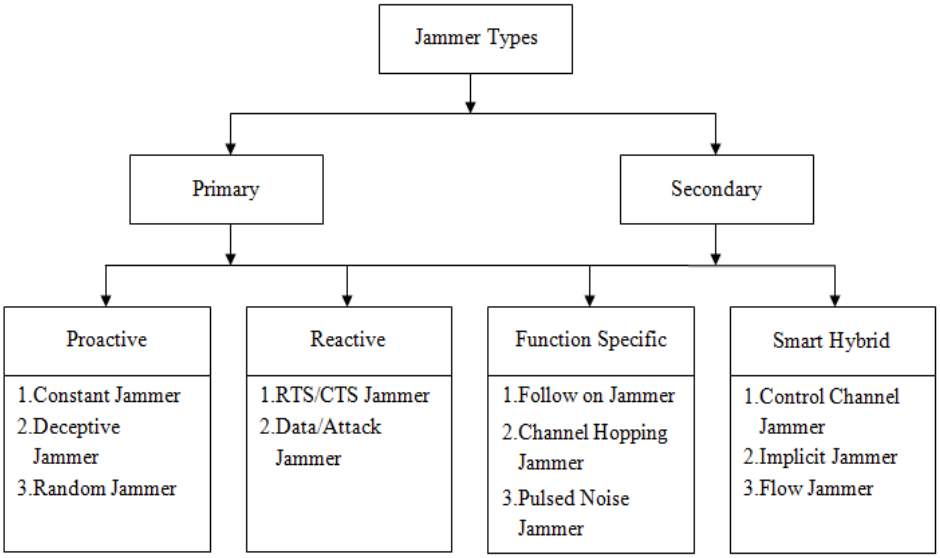


FIGURE 1. Wireless network jammer types.

overwhelm resources through Denial-of-Service (DoS) assaults, or carry out man-in-the-middle attacks [2]. Wireless Sensor Networks (WSN), which consist of numerous observation nodes spatially deployed to monitor a target plant or physical process, are particularly susceptible to these threats. A jammer can effectively interfere with legitimate communication by generating a jamming signal related to the transmit signal, especially when it can partially or completely obtain the transmit signal [3]. However, traditional constant jamming models, which continuously conduct JAs, are inefficient and energy intensive [4]. Instead, a malicious node can use its sensory ability to sense the wireless environment and effectively determine its jamming policy [5]. Physical-layer security provides perfect information-theoretic security by using the physical characteristics of wireless channels if the information rate of the legal users is greater than that of the eavesdroppers [6]. However, modeling and implementing security solutions in real-world Mobile Crowdsourcing Systems (MCS) is challenging. Artificial intelligence soft computing approaches are primarily used to address security issues due to the complexity of everyday problems involving them [8]. The effects of jamming are contingent on the modulation scheme, jamming-to-signal ratios, interleaving of a target system, and channel coding [7]. Figure 1 depicts the jammers of various wireless networks. Intentional interference over wireless signals is used to escalate DoS-attacks in wireless networks. When transmission error rates cannot be offset by error correction, usability is rejected in digital communications. On the modulation scheme, jamming-to-signal ratios, interleaving of a target system, and channel coding, the jamming effects are contingent. While jamming is typically addressed with an external threat model, adversaries with internal information of network secrets and protocol specifications can initiate low-effort JAs, which are difficult to detect and counter.

In addition to the threats and countermeasures, the introduction of GSM-based jammers and the Adaptive Neuro-Fuzzy Inference System (ANFIS) algorithm play a significant role in enhancing the security of wireless communications. GSM-based jammers are a type of intelligent jammer that specifically target GSM frequency bands used for mobile communications. Unlike traditional jammers that continuously emit interference signals, GSM-based jammers intelligently detect and disrupt GSM signals, making them more efficient and effective. They are designed to interfere with the communication link between a mobile phone and its base station, thereby preventing the establishment of a connection. This is achieved by transmitting a signal on the same frequency as the mobile phone, effectively drowning out the legitimate signal [23]. On the other hand, the ANFIS algorithm is a type of artificial intelligence algorithm that combines the reasoning capabilities of fuzzy logic systems with the learning capabilities of neural networks. This hybrid approach allows ANFIS to handle complex, nonlinear systems and make accurate predictions or decisions based on a set of inputs. In the context of wireless communications, ANFIS can be used to distinguish between legitimate signals and jamming signals, thereby improving the efficiency and effectiveness of the jamming process. It does this by applying a set of fuzzy "if-then" rules to the input data, and then using a neural network to learn and adapt these rules based on the data it receives [17]. Together, GSM-based jammers and the ANFIS algorithm provide a robust and intelligent solution for securing wireless communications against various types of attacks. This paper puts forth a proposal for an intelligent mobile phone jammer leveraging GSM technology

and evaluates its design in comparison with other intelligent algorithms.

To elevate DoS-attacks in wireless networks, intentional interference over wireless signals is used as a catalyst. Jamming is typically addressed with an external threat design. However, low-effort Jas, which are challenging to detect and defeat, are initiated by adversaries with internal information of network secrets and protocol specifications [9]. A wide variety of behaviors were utilized by jammers to generate DoS. Numerous jamming prototypes and hypotheses can be exhibited in the jamming literature [10]. Different types of wireless JAs, such as sensing- and random-centered jamming, can be launched; their effects can be detrimental to network performance [11]. Jamming is effective in MANET along with interfering in legal communication. The idle channel requisite for sending packets is unidentified by the sender. All the packets sent were not received by the receiver, even if the packets had been sent successfully. This is caused by the attacker who disregards the communication protocol along with results in low PDR [12]. A WSN JA occurs without the perpetration of specialized hardware or software and it is found catastrophic. Passive listening to the wireless media transmitted on a similar frequency band as the legal transmitting signal could be used to carry it out. Higher energy efficacies, decreased detection probability, along with anti-jamming resistance are typical JA's traits [13], [21], [23]. The state estimator is averted as of receiving or using a particular measurement by any adversarial activity known as jamming. Different practical methods, encompassing GPS spoofers, wireless jammers, together with coordinated DoS attacks, can be utilized to conduct jamming. Although preventing JAs is difficult, it is possible to lessen their effects [14], [15], [16].

The remainder structure of this paper is as follows: Section II discusses related works. Section III delves into the specifics of the proposed intelligent mobile phone jammer design. Section IV elaborates on the results obtained from the deployment of the proposed design and discusses them in detail. Finally, Section V wraps up the paper and suggests areas for future exploration

II. LITERATURE REVIEW

Shitharth and Prince Winston [18] suggested the Hierarchical Neuron Architectures-centric Neural Network (HNA-NN) together with the Intrusions Weighted Particle-centric Cuckoo-Search Optimizations (IWP-CSO) methodology. Centered on the optimization, detecting along with classifying the intrusions in a SCADA network was the main intention. Grounded on sensitivity, false detection rates, precision, recall, specificity, accuracy, Jaccard, and Dice, the system's performance was appraised by the experiential outcomes.

Moon et al. [19] recommended an Intrusion Detection (ID) system to detect APT attacks grounded on a decision tree employing behavior information examination that was rationally altered after intrusion in a system. Grounded on behavior information, the network process along with its behavior was examined by the recommended system to learn via decision tree and detected intrusion. By executing quick detection as of APT attacks, a diminished damage size was supported by a recommended system that occurred newly along with prevailing malware.

Mishra et al. [20], determined the cause of issues associated with disparate Machine Learning (ML) techniques in spotting intrusive activities by executing a detailed examination of disparate ML methodologies. Corresponding to every attack, the i) attack classification along with ii) mapping of attack features were proffered. Regarding detection competency, the attack's categories were spotted by examining along with contrasted the ML techniques centered on their detection competency.

Yin et al. [21], recommended the RNN-IDS prototype for ID that had high accurateness in the binary along with multi-class classification. Particularly under the multi-class classification of the NSLKDD data set, a higher accuracy together with detection rates with the lower false-positive rate was attained when analogized with the prevailing classification methodologies, like the random forest, J48, and naive Bayesian. The ID's accuracy along with competency for intrusion type recognition was effectually augmented by this prototype.

Ashfaq et al. [22], intended an SSL algorithm by probing a divide-and-conquer framework for augmenting the classifier's performance on ID data sets. Here, grounded on fuzziness, the unlabeled samples along with predicted labels were categorized. The base classifier utilized was the NN with Random weights (NNRw) because it was computationally effective along with pre-eminent learning performance. An independent coupled with an arbitrary selection of concealed-node parameters in NNRw was eventuated. After determining the association betwixt the fuzziness generated by the classifier on a cluster of samples, attaining the better classification accurateness was limited along with their misclassification rates.

III. PROPOSED INTELLIGENT MOBILE PHONE JAMMER DESIGN

A. ATTACK DETECTION AND PREVENTION SYSTEM USING ADAPTIVE NEURO-FUZZY INTERFERENCE SYSTEM CLASSIFIER

A new type of intelligent mobile phone jammer design, based on GSM, is introduced to address the limitations of current conventional jammers. This jammer uses the Adaptive Neuro-Fuzzy Inference System (ANFIS) to detect jamming signals, leveraging the neural network's reasoning, and learning capabilities and applying fuzzy ''if-then'' rules. The system is built on the Divide and Conquer (DAC) and Received Signal Strength Indicator Transmit Power Control (RSSITPC) algorithms. The Jamming Attack (JA) is then evaluated using Packet Sending Rate (PSR) and Packet Delivery Rate (PDR). Subsequently, the Hybrid-CLRA Scheme is employed to identify attacks. ANFIS then classifies the data into two

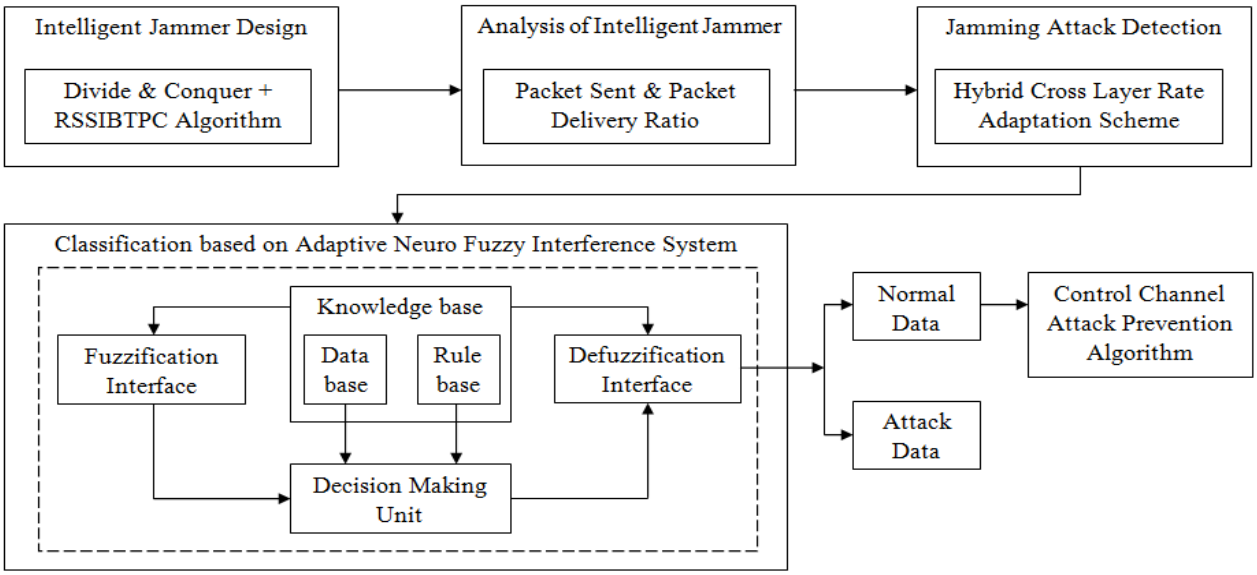


FIGURE 2. Architecture of ANFIS classification-based jamming attack detection.

types: normal data and attack data. The normal data is safeguarded from attacks using the Cross-layer Collaborative Attack Prevention (CCAP) algorithm. The architecture design, as shown in Figure 2, provides a detailed explanation of this proposed work.

To tackle the downsides of prevailing conventional intelligent mobile phone jammer, a GSM-based intelligent mobile jammer is engendered here. The reasoning mechanism and learning ability of the neural network are utilized by the ANFIS to identify the presence of jamming signal by applying fuzzy "if-then" rules. It is grounded on the Divide and conquers (DAC) and RSSITPC algorithms. The JA is then examined using PSR and PDR. In the end, the Hybrid-CLRA Scheme is utilized to detect attacks. Finally, the data is classified into two categories: attack data and normal data, by the ANFIS [17]. The normal data is protected against attacks by the CCAP algorithm. Moreover, the architecture design evinced in Figure 2 is utilized to elucidate this proposed work in detail.

B. MECHANISMS OF EFFECTIVE GSM-BASED INTELLIGENT JAMMING

Jamming aims to inject an interference signal into the transmission frequency, overpowering the original signal and preventing it from being received at the other end. It's important to note that jamming can't completely block the transmission. Successful jamming results in the denial of the communication transmission's usage. For effective jamming, the power of the jammer should be approximately equal to the signal power at the receiver. In digital communications, usability is denied when transmission error rates can't be compensated by error correction. The effects of jamming depend on the modulation scheme, jamming-to-signal ratios, interleaving of a target system, and channel coding. If high jamming efficiency is required, a higher Jammer Effective Radiated Power should be provided. The concept of a GSM-based intelligent jammer is illustrated in Figure 3. Compared to a traditional jammer design, this design includes an intelligent jammer system, a circuit interface, a power unit, a power detector, and a GSM scanner.

The Divide and Conquer (DAC) based Received Signal Strength Indicator Transmit Power Control (RSSITPC) algorithm is introduced. DAC is used to distinguish the jamming signal from the legitimate signal by comparing the voltage in the received signal, as shown in Figure 4. This algorithm uses RSSI values to determine the appropriate transmission powers for neighboring nodes and dynamically adjust the transmission power. By reducing total energy consumption, the Transmission Power Control Algorithm improves the Packet Delivery Rate (PDR) performance and throughput, extending the sensor node's lifespan and reducing interference between transmitting nodes. According to this algorithm, each node uses the RSSI value to determine the appropriate transmission power for its neighbors. This algorithm dynamically adjusts the transmission power in response to environmental changes. Furthermore, the higher Jammer Effective Radiated Power should be provided if the jamming efficiency is requisite, which is evaluated as follows.

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \tag{1}$$

P_j = Jammer power
G_{jr} = Antenna gain from the jammer to receiver
G_{rj} = Antenna gain from receiver to jammer
R_{tr} = Range between communication transmitter and receiver
B_r = Communication receiver Bandwidth

L_r = Communication Signal Loss
P_t = TransmitterPower
G_{tr} = Antenna gain from transmitter to receiver
G_{rt} = Antenna gain from Receiver to transmitter
R_{jr} = Range between Jammer and Communication receiver
B_j = Jammer Bandwidth
L_J = Jamming signal loss

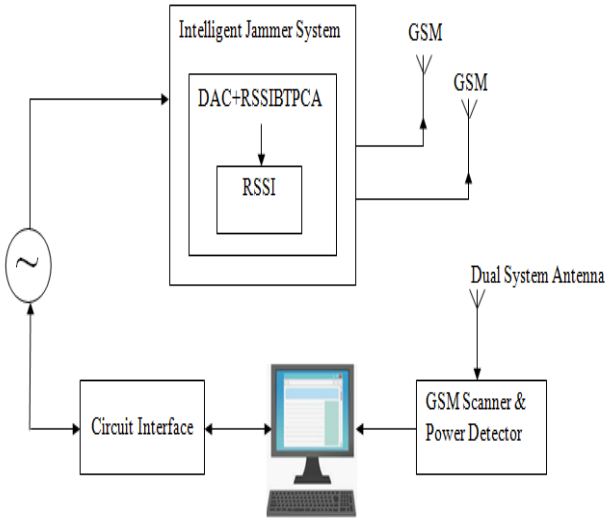


FIGURE 3. GSM based intelligent jammer design.

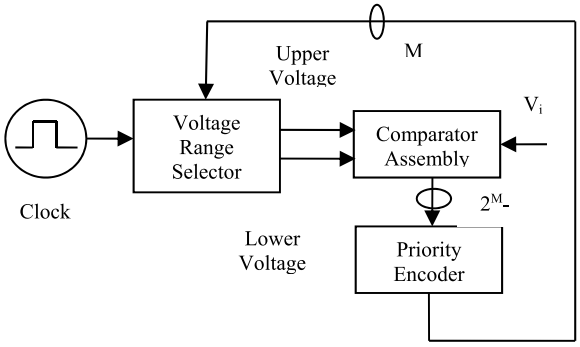


FIGURE 4. ISAR-ADC based on divide & conquer algorithm.

The GSM-centric intelligent jammer concept is expounded in Figure 3. When analogized to a traditional jammer design, the jammer design encompasses an intelligent jammer system, a circuit interface, a power unit, a power detector, and a GSM scanner. The DAC-centered RSSITPC algorithm is now put forth. The DAC is used to identify the jamming signal form the legitimate signal by comparing the voltage in the received signal as shown in Figure 4. For determining the appropriate transmission powers for its neighbor's node along with dynamically modifying the transmission power, the RSSI values are employed in this algorithm. By reducing total energy consumption, the Transmission Power Control Algorithm augments PDR's performance and throughput which also extends the sensor node's life. The interference betwixt transmitting nodes is also diminished. The appropriate transmission power for its neighbors was determined by the RSSI value utilized by each node, according to this algorithm. With the environmental change, the transmission power is dynamically tuned by this algorithm.

C. TYPES OF JAMMERS AND THEIR ANALYSIS

There are various types of jammers, including reactive, deceptive, constant, and random jammers. These jammers typically operate by continuously emitting RF signals with the aim of entirely blocking legitimate traffic. It's important to note that all Jamming Attacks (JAs) generally do not adhere to MAC protocols.

Jammers disrupt wireless communications either by blocking a legitimate traffic source from a packet sender or by preventing the reception of legitimate packets. Following the deployment of a jammer, the next step is to analyze its impact. This is done using metrics such as Packet Sending Rate (PSR) and Packet Delivery Rate (PDR) to evaluate the jammer's effectiveness.

1) PACKET SEND RATIO (PSR)

By tracking the whole packets that are delivered effectively by the source and those which intended to send to a MAC layer, the wireless device gauges. The PSR is when has to send messages. By the MAC layer of Transmitter, packets to be transmitted are assumed. But, owing to jamming interference just of such packets could be transmitted in time. is computed as

$$PSR = \frac{P}{Q} = \frac{Packets\ sent}{Packets\ Intended\ to\ be\ sent} \tag{2}$$

The jammer's efficacy over a transmitted is depicted by PSR. The main medium access is the carrier sense employed here. The medium is put in a busy state by jamming signals with carrier sensing. The queues of transmission would consequently get filled rapidly. Dropping will occur in the packet that enters the totally occupied queue.

2) PACKET DELIVERY RATIO (PDR)

The wireless device readily gauges the PDR. The proportion of packets effectively received by a destination to the total packets sent by the sender indicted the PDR. It is denoted as 0 if no packets are received. Consider, packets as of a transmitter received by . However, only as of these packets were sent to the (Receiver) higher layers effectively. It is pondered as the successful reception, only if the CRC (i.e. Cyclic Redundancy Codes) check is successfully passed by the packet. The JA's effectiveness over Rx is captured by the which is a contrast to. The is computed as (if then is pondered as zero):

$$PDR = \frac{U}{V} = \frac{Packets\ Received}{Packets\ sent\ to\ it} \tag{3}$$

D. INTEGRATING A HYBRID CROSS-LAYER RATE ADAPTATION SCHEME FOR JAMMING DETECTION

This work employs a Hybrid Cross-Layer Rate Adaptation (CLRA) scheme to detect Jamming Attacks (JA). Jamming detection is typically performed at the Physical (PHY) or Medium Access Control (MAC) layers, as it's often not feasible at higher layers. This protocol uses an upper-layer security technique based on the PHY layer, considering JA detection on both the PHY and MAC layers.

The proposed scheme dynamically adjusts the coding levels and modulations to maximize performance under varying wireless channel conditions. This allows for a higher data rate and maximum throughput using the CLRA Scheme. The primary concept of such systems is to assess the quality of the channel and adjust the data transmission mode accordingly. This is usually achieved using metrics collected at the sender, such as Signal Strength Indicator (SSI), Signal to Noise Ratio (SNR), probing packets, long-term data, and continuous losses or successes.

An easy approach to acquire crucial information about wireless channel conditions is to maintain statistics on data delivery, such as the retry ratio, Packet Error Rate (PER)/Bit Error Rate (BER), and the achieved long-term/short-term average throughputs. The channel quality-centric approach appraises the quality of the channel based on the measured SNR or SSI rather than the statistics. The data transmission mode is adjusted using a pre-defined threshold lookup table.

The strategy's cross-layer concept includes the Quality Adaptation Module (QAM) in the application layer and the Rate Adaptation Module (RAM) in the PHY and MAC layers. After determining the rate restrictions, the RAM informs the QAM, which then modifies the data quality transmitted to the receiver via the PHY and MAC layers. A novel rate adaptation mechanism is introduced in the RAM to improve the use of the wireless link. The proposed CLRA technique selects the data transmission mode based on wireless channel conditions.

E. INTEGRATING ADAPTIVE NEURO-FUZZY INFERENCE SYSTEM (ANFIS) IN JAMMING DETECTION

The Adaptive Neuro-Fuzzy Inference System (ANFIS) is a fuzzy model integrated into an adaptive framework, making ANFIS modeling more systematic and less dependent on specialized knowledge. This work uses the ANFIS Classifier model to detect the Jamming Attack (JA) depicted in Figure 5.

The ANFIS model, also known as the Neuro-Fuzzy Controller (NFC), maps inputs and outputs using corresponding Membership Functions (MF). The input parameters for the fuzzy logic are the signal strength of the received signal, error rate, learning signals and training data. The NFC predicts the output based on input features. The learning process adjusts both preceding and succeeding parameters using a combination of Backpropagation (BP) and least-squares estimate. The NFC modifies the input MF and output MF parameters based on the selected error situation.

The ANFIS adjustment parameter is illustrated in Figure 6. Here, a 5-layered Neural Network (NN) named ANFIS simulates the working principle of the fuzzy inference system. After loading all the ANFIS parameters, the ANFIS classifier identifies the MF, error rate, learning methods, and their corresponding attributes. The training approach continues until the altered input/output MF and corresponding parameters are defined. The ANFIS is then subjected to testing frameworks. This process continues until the rules and MFs are adjusted. Finally, the updated parameters and their modified attributes are saved in the ANFIS. The classifier is trained to achieve maximum classification accuracy.

The ANFIS structure is offered with '2' fuzzy if-then rules. The fuzzy membership grade is computed by equation (4). For example, if a bell-shaped MF is utilized, then 'a' is computed by equation (6). The layer-2 outputs are appraised as per equation (7). The outputs of layer-3 are appraised as per equation (8). The outputs of layer 4 are assessed by equation (9). The output of layer-5 is offered as per equation (10). Consequently, the ANFIS's output is gauged as per equation (11). By substituting equation (8) to equation (11), we get equation (12).

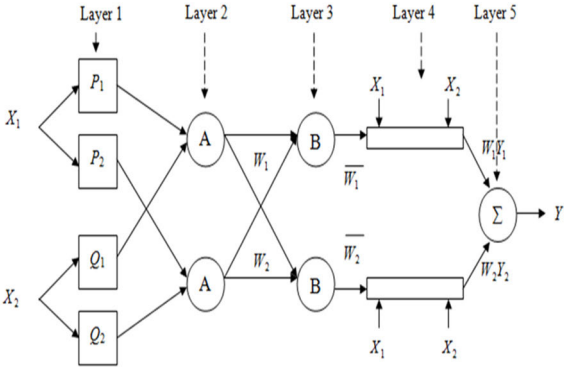


FIGURE 5. Structure of anfis classifier.

ANFIS adjustment parameter is delineated in figure 6. Here, the fuzzy inference system's working principle is simulated by a 5-layered NN named ANFIS. Initially, the MF, error rate, learning methods, along with their corresponding attributes are identified by ANFIS classifier after loading all the ANFIS parameters. The training approach is continued unless the altered input/output MF along with corresponding parameters is defined. Subsequently, the ANFIS is subjected to testing frameworks. This process is continued until the rules and MFs are adjusted. Finally, the updated parameters along with their modified attributes are saved in the ANFIS. The maximal classification accuracy is attained by training this classifier.

In the '5' layers, Adaptive nodes are encompassed in layer-1 and layer-4, while, the fixed nodes are included in layer-2, layer-5, and layer-3. Here, with '2' fuzzy if-then rules, the ANFIS structure is proffered as,

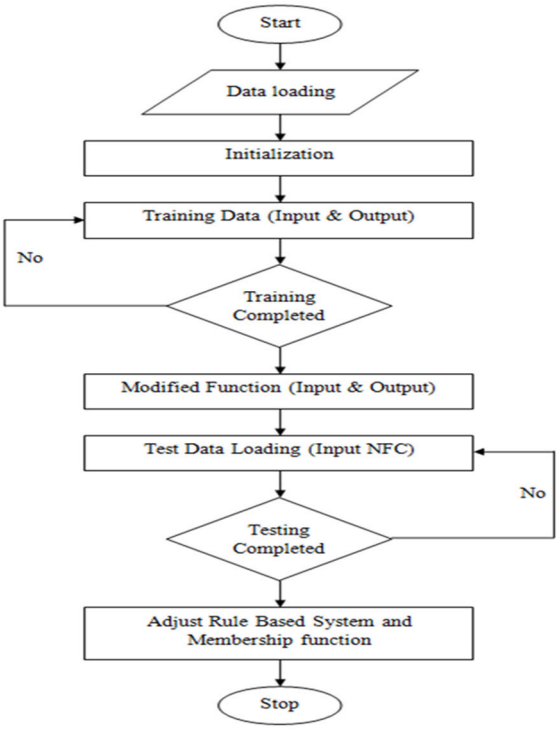


FIGURE 6. ANFIS classification flow chart.

Rule I: If $(X_1\ is\ P_1)\&(X_2\ is\ Q_2)$; $(F1 = p_1X + q_1Y + r_1)$
Rule II: If $(X_1\ is\ P_2)\ \&(X_2\ is\ Q_2)$; $(F2 = p_2X + q_2Y + r_2)$
where, the ANFIS's inputs are notated as $X_1\ and\ X_2$. The fuzzy sets are denoted by $P\ and\ Q$. Through the fuzzy part, the outputs defined by the fuzzy rule base are signified by F_i. During training, the designed parameters predicted are proffered by $p_i, q_i\ and\ r_i$. The fuzzy membership grade computed by equation (4) is indicated by the outputs.

$$O_i^1 = \mu_{Pi}(X_1) \quad i = 1, 2 \tag{4}$$

$$O_i^1 = \mu_{Qi-2}(X_2) \quad i = 3, 4 \tag{5}$$

where, any fuzzy MF was taken up by $\mu_{Pi}(X_1)$ and $\mu_{Qi-2}(X_2)$. For example: if a bell-shaped MF is utilized, then $\mu_{Pi}(X_1)$ is computed by (6)

$$\mu_{Pi}(X_1) = \frac{1}{1 + \left\{\left(\frac{X - u_i}{s_i}\right)^2\right\} t_i} \tag{6}$$

Here, the MF parameters pondered are $s_i, t_i\ and\ u_i$. In an easy multiplier, the nodes requisite to be presented in layer-2 are executed. The layer-2 outputs are appraised as,

$$O_i^2 = w_i = \mu_{Pi}(X_1)\,\mu_{Qi}(X_2) \quad i = 1, 2 \tag{7}$$

Fixed nodes, indicated as N are found in layer-3. Their normalization positions to the firing strengths (FS) are modeled as N from previous second layer. Here, the outputs are appraised as,

$$O_i^3 = \bar{w}_i = \frac{w_i}{w_1 + w_2} \quad i = 1, 2 \tag{8}$$

It is termed the normalized FS. Adaptive nodes are included in layer 4. An output attained by computing the product of the 1st-order polynomial and normalized FS is formed by each node. Hence, the outputs are assessed by

$$O_i^4 = \bar{w}_i F_i = \vec{w}_i (p_i X_1 + q_i X_2 + r_i) \quad i = 1, 2 \tag{9}$$

Only one fixed node, indicated as S is encompassed in layer-5 that summates the whole incoming signals. Thus, the output is proffered as,

$$O_i^5 = \sum_{i=1}^{2} \bar{w}_i F_i = \frac{\sum_{i=1}^{2} w_i f_i}{w_1 + w_2} \quad i = 1, 2 \tag{10}$$

Consequently, '2' adaptive layers containing layer-1 and layer-4 are contained in the ANFIS structural design. '3' changeable parameters $\{s_i, t_i, u_i\}$ are linked to the input MF's named as premise parameters, are comprised in layer-1. Concerning the 1st-order polynomial, '3' modifiable parameters $\{p_i, q_i, r_i\}$ are encompassed in layer-4 along with such parameters referred to as consequent parameters. Subsequently, the fuzzification process is executed by the fuzzifier. The ANFIS's output is gauged as,

$$F = \frac{w_1}{w_1 + w_2} F_1 + \frac{w_2}{w_1 + w_2} F_2 \tag{11}$$

Next, by substituting equation (8) to equation (11) as

$$F = \vec{w}_1 F_1 + \vec{w}_2 F_2 \tag{12}$$

The fuzzy "if-then rules" are utilized in the equation (12) which is expressed as,

$$F = \bar{w}_1 (p_1 X_1 + q_1 X_2 + r_1) + \bar{w}_2 (p_2 X_1 + q_2 X_2 + r_2) \tag{13}$$

The equation (13) denotes the linear combination of p_1, q_1, r_1, p_2, q_2 and r_2 (i.e. consequent parameters).

F. ENHANCING WIRELESS NETWORK SECURITY THROUGH CONTROL CHANNEL COORDINATION AND EVASION TECHNIQUES

In a wireless network, the control channel coordinates channel utilization, enhancing network capacity using multiple channels. To prevent Jamming Attacks (JA), a control channel composed of several clusters is proposed, each maintaining its own control channel with a unique hopping sequence. A higher-level network jammer can jam the control channel by exploiting information about cryptographic quantities and protocol procedures from compromised nodes. The evasion entropy metric is used to measure a jammer's capability to accurately predict the future control channel based on previously observed data. Compromised nodes are identified by calculating the Hamming distance between the jammer's hop sequence and the original hop sequence. Once these nodes are identified, the control channel, which uses frequency hopping, is re-established by updating the hopping sequence. The evasion delay, which measures the latency associated with

the successful reestablishment of the new control channel, is also considered. Furthermore, the evasion ratio provides an indication of the presence of communications, particularly in the context of jamming availability.

IV. TEST BED CONFIGURATION

The testing environment is developed as shown in the figure 7. The top portion if the circuit is meant for the power supply that manages the power requirement for our jammer design. The bottom left is the Intermediate Frequency (IF) generator with is used to infuse the noise with the RF signal to make it look like an interference randomly created in the environment to the receivers. Last PCB is for RF signal generator used to produce actual jamming signals.

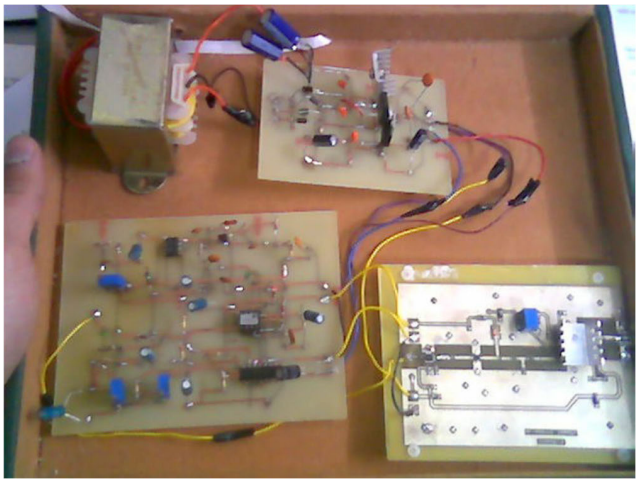


FIGURE 7. GSM Jammer construction.

V. RESULTS AND DISCUSSION

The proposed JA Detection and Prevention System's performance, as well as experimental analysis, are appraised in this section.

A. PERFORMANCE MEASURES

By the terms "True Positive (TP)", "False Positive (FP)", "True Negative (TN)" and "False Negative (FN)", the error rates are commonly described as,

TP: the classification result is positive in the JA's existence.

TN: the classification result is negative in the JA's nonappearance.

FN: the classification result is negative in the JA's existence.

FP: the classification result is positive in the JA's nonappearance.

The ANFIS Classifier's Specificity, Accuracy, and Sensitivity are computed by utilizing the above metrics,

$$Sensitivity = \frac{True\ Positive}{True\ \ Positive + False\ Negative} * 100\% \quad (14)$$

$$Specificity = \frac{True\ Negative}{True\ \ Negative + False\ Positive} * 100\% \quad (15)$$

$$Detection\ Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \times 100\% \quad (16)$$

TABLE 1. Analysis of jamming effectiveness for different service providers (based on BCCH frequencies and MS is in in- call case).

Metric	Constant Jammer		Reactive Jammer	
	TP Rate (%)	TN Rate (%)	TP Rate (%)	TN Rate (%)
Noise	65.2	76.4	0	0
CBR	78.5	82.2	76	66.3
PDR	80	88.1	69	88
Max. IT	84.5	74.9	73.5	72.6
JSR	75	80	76.7	78.1
Dt	77.3	83.4	80	83
SP	80.1	86	86.2	79.5
Sv.Pvr	76.2	80.2	75	78.4
FB	78	79.9	78.3	76.8
ARFCN	79.3	80.6	73.5	80.9

The mobile can be jammed only after the ongoing call is disconnected. The various metrics considered for jamming are mentioned in the Table 1.

TABLE 2. Jamming effectiveness of various frequency bands.

Freq. band/ network	MS status	Distance	Jamming effectiveness	J/S
938.2-941.3 (IDEA)	Call in progress	30 m	Not effective	**27**
935-941.3 (IDEA)	Call in progress	30 m	Effective	**25**
948.2-951.2 (BSNL)	Call in progress	30 m	Not effective	**13**
947-960(BSNL)	Call in progress	30 m	Not effective	**11**
941.4-944.4 (AIRTEL)	Call in progress	30 m	Not effective	**30**
941.4-957 (AIRTEL)	**Call in progress**	**30 m**	**Not effective**	**25**

Various frequency bands together with their effectiveness are elucidated in Table 2. Frequency bands of IDEA, BSNL, and AIRTEL, Jamming effectiveness, Jamming-to-Signal Ratio, Mobile station status, Distance, along with the network's remarks are exhibited in the above table.

When analogized with conventional classification models like NN and KNN, higher values of Specificity, Accuracy, and Sensitivity were attained by the proposed ANFIS, which was delineated in table 2. 97.6% sensitivity, 96.3% Specificity, and also 98.67% Accuracy was attained by the proposed ANFIS when contrasted to other prevailing schemes.

TABLE 3. Performance table for classification.

Performance Measures	Sensitivity	Specificity	Accuracy
Proposed ANFIS	97.6%	96.3%	98.67%
NN	94.3%	95.3%	91.8%
KNN	96.2%	91%	95.7%

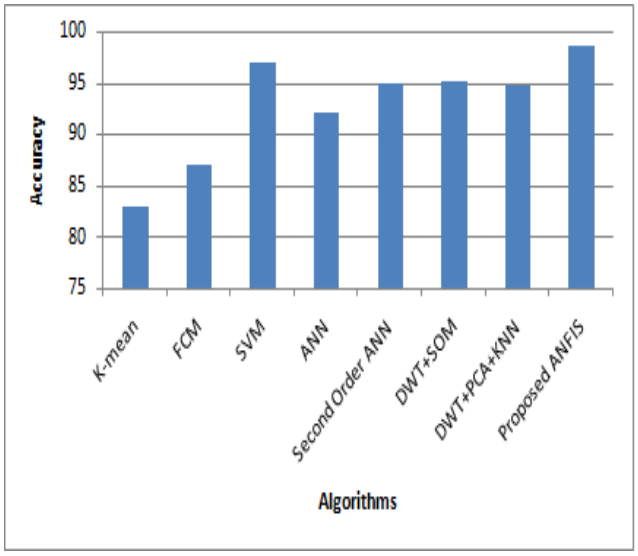


FIGURE 8. Comparison of the existing and the proposed technique in terms of accuracy.

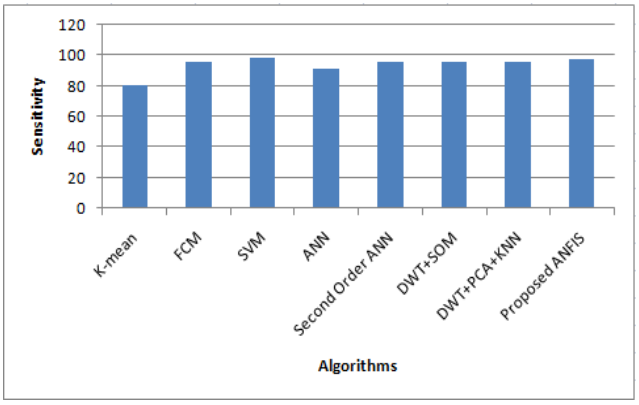


FIGURE 9. Comparison of the existing and the proposed technique in terms of sensitivity.

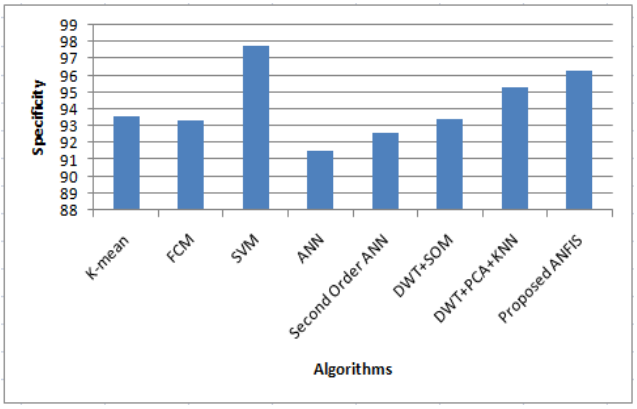


FIGURE 10. Comparison of the existing and the proposed technique in terms of specificity.

The effectiveness of the jammer increases when the mobile device is moving away for the cell tower and vice versa. Regarding accuracy, the proposed ANFIS classifier is analogized with prevailing K-Mean, FCM, SVM, ANN, Second-order ANN, DWT+SOM, DWT+PCA+KNN classifier, which is signified in figure 8. When analogized with the ANFIS classifier, the prevailing algorithms depicted a low accuracy. For both the proposed and the prevailing classifier, the accuracy is elevated as the number of data increases. It is inferred that a higher performance was attained by the proposed classifier.

Regarding sensitivity, the proposed ANFIS classifier is analogized with prevailing K-Mean, FCM, SVM, ANN, Second-order ANN, DWT+SOM, DWT+PCA+KNN classifier, which is signified in figure 9. Normally, the measure of a number of actual positives exactly recognized is the sensitivity. Here, the sensitivity is elevated with elevation in the number of data. Greater performance is exhibited by the proposed one when analogized with the prevailing classifiers.

Regarding specificity, the proposed ANFIS classifier is analogized with prevailing K-Mean, FCM, SVM, ANN, Second-order ANN, DWT+SOM, DWT+PCA+KNN classifier, which is signified in figure 10. Usually, the number of actual negatives that are exactly recognized is measured as Specificity. The specificity value is too low for the prevailing classifier. Specificity increases with an increase in

TABLE 4. Analysis of path loss from BTS TO MS at different locations.

Distance (m)	Path loss in Urban	Signal at MS (dBm)	Path loss in Suburban	Signal at MS (dBm)	Path loss at Rural	Signal at MS (dBm)
100	-90.5	-54.5	-86.2	-47.2	-62.9	-20.9
200	-100	-64	-96.8	-57.8	-73.5	-31.5
300	-107	-71	-103	-64	-79.6	-37.6
400	-111.5	-75.5	-107	-68	-84	-42
500	-115	-79	-110.8	-71.8	-87.5	-45.5
600	-117.7	-81.7	-113	-74	-90.3	-48.3
700	-120	-84	-115	-76	-92.7	-50.7
800	-122	-86	-118	-79	-94.7	-52.7
900	-124	-88	-119.8	-80.8	-96.5	-54.5
1000	-125	-89	-121.4	-82.4	-98.18	-56.18
2000	-136	-100	-132	-93	-108	-66
3000	-142	-106	-138	-99	-114	-72

the number of data. The proposed ANFIS classifier exhibits greater performance for any number of data when contrasting the proposed along with prevailing classifiers.

The Path loss data is considered depending in the distance of the mobile stations to the cell tower (Base Transceiver Station, BTS). The geographical conditions also contribute the path loss because of the attenuating factors of the radio signals. In the rural areas fading and multi-path reflection are high due to the high rise buildings. Consider BTS antenna height is 30m, transmission (TX) power at the open region is 16W (42dBm), TX power at the suburban region is 8W (39dBm) and TX power at the urban region is 4W (36dBm). The path loss from BTS to MS is computed by using a HATA model and the values are given in Table 4.

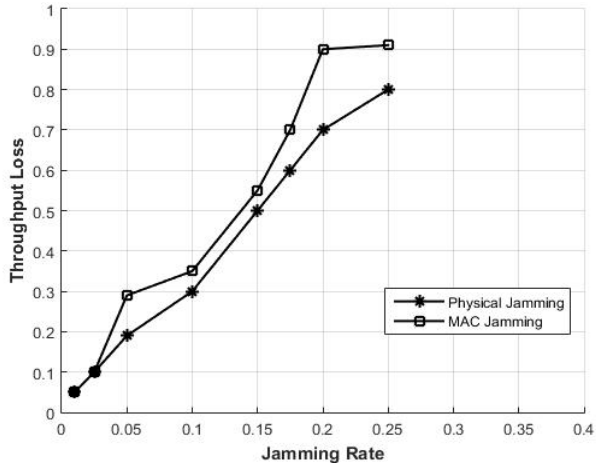


FIGURE 11. Effect of jammer rate on throughput loss.

The throughput losses under MAC and PHY jamming rates were delineated in figure 11. With the rise in jamming rate, a high diminish in the network throughput is specified in the plot. For a huge fraction of jamming rates, it is perceived that MAC layer jamming diminishes the network throughput 20-30% more than physical jamming.

VI. CONCLUSION

The ANFIS is proposed in this work to spot and mitigate the JA in the MAC and PHY layers. By employing DAC and RSSIBTPC Algorithm, the GSM grounded Effective Intelligent Jammer is modelled. The JA is analysed with the aid of PSR and PDR. Subsequently, the JA in the MAC and PHY layer is assisted by the Hybrid CLRA Scheme. The Normal and Attack data are classified into separate classes by the ANFIS classifier. Finally, the CCAP Mechanism executes the normal data prevention. Utilizing divergent performance metrics of Sensitivity (97.6%), Specificity (96.3%), and Accuracy (98.67%), the proposed classification technique is investigated in performance evaluation. Specifically, a higher threshold was attained by the ANFIS technique as of the comparison outcomes. This work is ameliorated in the future by adding JA prevention in more Network layers, along with hybridizing the ANFIS system with an advanced optimization algorithm to detect more attacks.

Funding: This research received no external funding.

Data Availability Statement: Data availability is mentioned in this manuscript.

Conflicts of Interest: There is no conflict of interest among the authors.

REFERENCES

[1] S. Amuru, C. Tekin, M. v. der Schaar, and R. M. Buehrer, "Jamming bandits—A novel learning method for optimal jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2792–2808, Apr. 2016.

[2] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6475–6488, Jul. 2017.

[3] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.

[4] S. T. Ahmed, V. V. Kumar, K. K. Singh, A. Singh, V. Muthukumaran, and D. Gupta, "6G enabled federated learning for secure IoMT resource recommendation and propagation analysis," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108210.

[5] X. Tang, P. Ren, and Z. Han, "Jamming mitigation via hierarchical security game for IoT communications," *IEEE Access*, vol. 6, pp. 5766–5779, 2018.

[6] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, "Secure cooperative transmission against jamming-aided eavesdropper for ARQ based wireless networks," *IEEE Access*, vol. 5, pp. 3763–3776, 2017.

[7] L. Xiao, D. Jiang, D. Xu, W. Su, N. An, and D. Wang, "Secure mobile crowdsensing based on deep learning," *China Commun.*, vol. 15, no. 10, pp. 1–11, Oct. 2018.

[8] Camelia-M. Pintea, P. C. Pop, and I. Zelina, "Denial jamming attacks on wireless sensor network using sensitive agents," *Log. J. IGPL*, vol. 24, no. 1, pp. 92–103, Feb. 2016.

[9] G.-H. Lee, J. Jo, and C. H. Park, "Jamming prediction for radar signals using machine learning methods," *Secur. Commun. Netw.*, vol. 2020, pp. 1–9, Jan. 2020.

[10] K. M. K. Raghunath, V. V. Kumar, M. Venkatesan, K. K. Singh, T. R. Mahesh, and A. Singh, "XGBoost regression classifier (XRC) model for cyber attack detection and classification using inception v4," *J. Web Eng.*, pp. 1295–1322, Apr. 2022.

[11] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," *IEEE Secur. Privacy*, vol. 14, no. 1, pp. 47–54, Jan. 2016.

[12] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 1, pp. 2–14, Mar. 2019.

[13] L. Mokdad, J. Ben-Othman, and A. T. Nguyen, "DJAVAN: Detecting jamming attacks in vehicle ad hoc networks," *Perform. Eval.*, vol. 87, pp. 47–59, May 2015.

[14] O. Osanaiye, A. Alfa, and G. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 18, no. 6, p. 1691, May 2018.

[15] H. Zhu, C. Fang, Y. Liu, C. Chen, M. Li, and X. S. Shen, "You can jam but you cannot hide: Defending against jamming attacks for geo-location database driven spectrum sharing," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2723–2737, Oct. 2016.

[16] P. Iyappan, J. Loganathan, M. Kumar Verma, A. Dumka, R. Singh, A. Gehlot, S. V. Akram, S. Kaur, and K. Joshi, "A generic and smart automation system for home using Internet of Things," *Bull. Electr. Eng. Informat.*, vol. 11, no. 5, pp. 2727–2736, Oct. 2022.

[17] M. Hatamzad, G. P. Pinerez, and J. Casselgren, "Addressing uncertainty by designing an intelligent fuzzy system to help decision support systems for winter road maintenance," *Safety*, vol. 8, no. 1, p. 14, Feb. 2022.

[18] S. Shitharth, "An enhanced optimization based algorithm for intrusion detection in SCADA network," *Comput. Secur.*, vol. 70, pp. 16–26, Sep. 2017.

[19] D. Moon, H. Im, I. Kim, and J. H. Park, "DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks," *J. Supercomput.*, vol. 73, no. 7, pp. 2881–2895, Jul. 2017.
[20] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 686–728, 1st Quart., 2019.
[21] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.
[22] R. A. R. Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, "Fuzziness based semi-supervised learning approach for intrusion detection system," *Inf. Sci.*, vol. 378, pp. 484–497, Feb. 2017.
[23] S. Sivaprakash and M. Venkatesan, "A design and development of an intelligent jammer and jamming detection methodologies using machine learning approach," *Cluster Computing*, vol. 22, pp. 93–101, Jul. 2019, doi: 10.1007/s10586-018-2822-7.

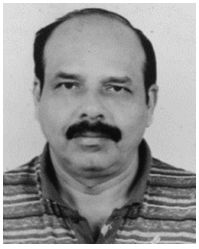
S. SIVAPRAKASH (Member, IEEE) received the Ph.D. degree in information and communication engineering from Anna University, Chennai, and the Master of Engineering degree in computer science and engineering. He is currently an Assistant Professor (Senior Grade) with the Vellore Institute of Technology, Vellore, India. He is also a Life Member of ISTE. He has more than ten publications to his credit in reputed international/national journals and conferences. His recent research interests include cloud computing, cyber security, and networks and its security. He has also written chapter in the book titled *Cloud Computing With Wireless Network and Pattern Recognition*.

U. V. ANBAZHAGU received the Ph.D. degree in big data analytics. She is currently an Assistant Professor with the Department of Computing Technologies, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chennai. Her research interests include artificial intelligence and machine learning.

IYAPPAN PERUMAL received the B.E. degree in computer science and engineering from the Krishnasamy College of Engineering & Technology, Anna University, in 2005, the M.Tech. degree in computer science and engineering from SMVEC, in 2008, and the Ph.D. degree from the Department of Computer Science and Engineering. He is currently an Senior Assistant Professor with the School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. He has published 20 research articles indexed in SCOPUS/SCI/UGC care journals. His research interests include service oriented architecture, service interoperability, and security in interoperation and web technologies. He is a Life Member of ISTE. He received the Gold Medal from Pondicherry University.

V. VINOTH KUMAR (Member, IEEE) is currently an Associate Professor with the School of Computer Science Engineering and Information Systems (SCORE), Vellore Institute of Technology (VIT), Vellore, India. He is the author/coauthor of papers in international journals and conferences, including SCI indexed papers. He has published as over than 60 papers in IEEE Access, Springer, Elsevier, IGI Global, and Emerald. His current research interests include wireless networks, the Internet of Things, machine learning, and big data applications. He is also an Associate Editor of *International Journal of e-Collaboration* and *International Journal of Pervasive Computing and Communications* and an editorial member of various journals.

T. R. MAHESH (Senior Member, IEEE) is currently an Associate Professor and the Program Head of the Department of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bengaluru, India. He has to his credit more than 40 research articles in Scopus and SCIE indexed journals of high repute. He has been an editor for books on emerging and new age technologies with publishers like Springer, IGI Global, and Wiley. He has served as a reviewer and a technical committee member for multiple conferences and journals of high reputation. His research interests include image processing, machine learning, deep learning, artificial intelligence, the IoT, and data science.



SURESH GULUWADI (Member, IEEE) is currently an Associate Professor with Adama Science and Technology University, Adama, Ethiopia, With nearly two decades of experience in teaching, his areas of specialization include pervasive computing, artificial intelligence, the IoT, data science, and WSN. He has five patents in IPR and has published approximately more than ten papers in reputed international journals. He has authored "Response Time Optimization in Wireless Sensor Networks." He has published numerous papers in national and international conferences and has served as an editor/reviewer for Springer, Elsevier, Wiley, IGI Global, Emerald, and ACM. He is an active member of ACM, I.E.(I), IACSIT, and IAENG. He has organized several national workshops and technical events.