scientific reports

Check for updates

OPEN

Malicious user classification in cognitive 5G networks using novel improved bidirectional encoder representations from transformers model

Saranya S.[1]✉, N. Malligeswari[2], F. Twinkle Graf[3] & V. Murugan[4]

In cognitive 5G networks, identifying malicious users is essential for protecting dynamic spectrum access against attacks like jamming as well as spectrum sensing fraud. However, the complexity associated with many 5G settings, limited labelled information, as well as evolving attack methods make it extremely challenging to detect these individuals. In order to provide dependable effectiveness as well as confidence in cognitive radio-enabled 5G communication frameworks, these networks need real-time, efficient, and adaptable classification approaches that can reduce false alarms while generalizing successfully. Therefore, this paper performs the Malicious User Classification in Cognitive 5G Networks (MUC-C5GN) using novel intelligent machine learning-oriented optimization methodology. The data is first collected from the standard benchmark sources called 5G Network Intrusion Detection Dataset (5G-NIDD). The pre-processing of this collected data is accomplished by the normalization and scaling methods. Next, the feature extraction of this pre-processed data takes place by the Self-Attention RNN-AE (Recurrent Neural Network-Autoencoder) approach. Finally, the classification of the malicious users in cognitive 5G networks is performed by the novel Improved Bidirectional Encoder Representations from Transformers (IBERT) model. The parameter tweaking in BERT is done by the nature inspired optimization algorithm called Revolution Optimization Algorithm (ROA). Accuracy maximization is considered as the fitness function for the overall MUC-C5GN model. Over seven types of attack as well as benign traffic, the proposed IBERT-ROA method is evaluated against LSTM-GRU, MLP, Chaotic DBN, and Detectron2 +YOLOv7. According to simulation results, IBERT-ROA achieves the best results with 99.74% accuracy, 98.48% sensitivity, 98.91% precision, 97.82% MCC, as well as 98.91% specificity—demonstrating improvements of up to 5.99% in sensitivity and 2.74% in accuracy over the state-of-the-art technique. These results demonstrate the effectiveness, scalability, as well as suitability of IBERT-ROA for real-time malicious user detection in dynamic cognitive 5G environments.

Keywords Cognitive 5G networks, Malicious user classification, Normalization and scaling, Self-Attention recurrent neural Network-Autoencoder, Improved bidirectional encoder representations from transformers, Revolution optimization algorithm

In recent times, 5G networks have changed the concept of dynamic access to spectrum through Cognitive Radio (CR) that enables secondary users to import opportunistically on unused spectrum bands[1]. As well as satisfying the ultra-reliable, low-latency communication services of 5G, this advanced method enhances spectral efficiency[2]. However, due to the fact that the cognitive radio configurations are not only open, but also

[1]Department of Computer Science and Engineering, Dr. N.G.P. Institute of Technology, Coimbatore 641048, India. [2]Department of Electronics and Communication Engineering, Easwari Engineering college, Chennai, Ramapuram 600089, India. [3]Department of Computer Science and Engineering (Data Science), Madanapalle Institute of Technology & Science, Madanapalle 517325, India. [4]Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi 600062, India. ✉email: ssaranya065@gmail.com

decentralized, the network becomes susceptible to various security vulnerabilities and in this case, malicious parties tend to exploit them[3]. In their effort to gain unauthorized access, these attackers can also: carry out DoS attacks, masquerade out spectrum sensing data or impersonate authorized users[4]. Consequently, the integrity, reliability, and effective functioning of cognitive 5G architectures would rely on the ability to identify and identify malicious activities in real-time[5].

Although machine learning methods and even signal processing methods have existed, there exist various limitations to the detection of malicious users in the 5G cognitive network[6]. To begin with, malicious activities are not easy to model once through a rule-based system because they are usually both dynamic and modifiable[7]. To prevent detection, attackers may replicate the activities of authentic users or utilize advanced methods like jamming, main user emulation or use Spectrum Sensing Data Falsification (SSDF)[8]. Second, classification models have access to a limited amount of labelled data, especially in real-world 5G network where data sharing is limited both by privacy issues and deployment limitations[9]. This limitation in resources may impede the efforts of developing not only robust but also generalizable methodology[10]. Third, efficient extraction and indeed categorization by any measure are further complicated by understanding the highly dynamic nature and the highly variable environments in which cognitive 5G networks have to deal with different traffic spectrum, user mobility and indeed signal conditions[11].

New and flexible classification techniques, capable of adapting to the changing nature of attacks and network bandwidth requirements are required to deal with such issues[12]. To avoid incorrectly classifying real users, methods must be able to learn from sparse, unbalanced, or noisy datasets while lowering false positives[13]. Moreover, for real-time execution on devices with restricted resources, minimizing computational overhead is essential[14]. The development of scalable, interpretable, as well as accurate classifiers for identifying malicious users describes a crucial component of safeguarding the future of cognitive 5G networks due to ongoing research in this field[15].

Conventional machine learning algorithms (like ELM, SVM, as well as DTs) and deep learning ensembles as well as incremental learning are some of the previous approaches for identifying malicious users in cognitive 5G networks. Even while ELM offers efficient generalization as well as rapid training, it struggles to adapt to rapidly changing network conditions and is very susceptible to damaging input interference. Although deep learning ensembles increase robustness, their deployment on edge devices—which are ubiquitous in 5G settings—is limited by their high processing needs as well as inference delays. While methods such as Self-Attention RNN-AE improve temporal feature learning, they can be computationally demanding as well as their efficacy can be diminished by noisy or incorrectly calibrated training datasets. Although incremental learning techniques adapt to evolving threats, they run the risk of catastrophic forgetting as well as decreased accuracy when update streams contain hostile or mislabeled information.

These issues are directly addressed by the proposed MUC-C5GN methodology through a combination of design choices: (i) IBERT for efficient bidirectional sequence modelling with integer quantization as well as reduced attention complexity—decreasing latency and memory usage for edge implementation; (ii) Self-Attention RNN-AE for extracting noise-resistant temporal–contextual features from diverse traffic patterns; and (iii) ROA optimization for dynamic fine-tuning to improve accuracy while maintaining low false positives, even in the face of class imbalance. This integration directly addresses the computational as well as adaptability constraints of previous attempts, allowing the framework to achieve increased detection accuracy while maintaining scalability and real-time viability. The diagram describing the system model for the Cognitive 5G network malicious users is displayed in Fig. 1.

The paper contribution is as below.

- To perform the MUC-C5GN using novel intelligent machine learning-oriented optimization methodology by gathering the 5G-NIDD dataset.
- To accomplish the pre-processing of this collected data by the normalization and scaling methods and to do the feature extraction by the Self-Attention RNN-AE approach.
- To perform the classification of the malicious users in cognitive 5G networks by the novel IBERT model, where the parameter tweaking in BERT is done by the nature inspired optimization algorithm called ROA that in turn considers accuracy maximization as the fitness function for the overall MUC-C5GN model.

The paper organization is as follows. Section 1 is the introduction of malicious users in cognitive 5G networks. Section 2 is literature survey. Section 3 is proposed methodology with proposed model, dataset description, pre-processing by normalization and scaling, feature extraction by self-attention RNN-AE, classification by novel IBERT and ROA algorithm. Section 4 is results and analysis. Section 5 is conclusion.

Motivation

Cognitive radio networks are essential for increasing spectrum efficiency as well as enabling dynamic spectrum access in the emerging field of 5G communication. However, because these networks are open as well as decentralized, they are particularly vulnerable to malicious user attacks, such as impersonation, jamming, and manipulation of spectrum sensing information. These risks compromise the dependability as well as security of crucial communication services in addition to impairing network effectiveness. Conventional detectors may have a problem with accuracy too, not to mention time adaptation, particularly when the wireless environment is highly dynamic and diverse (as it will be in the case of 5G). This vibrates an urgent need to develop smart, scalable and also good methods capable of catching evil users with the least amount of false positives. Operation of cognitive 5G networks requires the generation of trust in spectrum access options in addition to protection of the authorized users against misuse. These issues have to be resolved when developing next-generation wireless communication architectures that are reliable, secure, and robust.

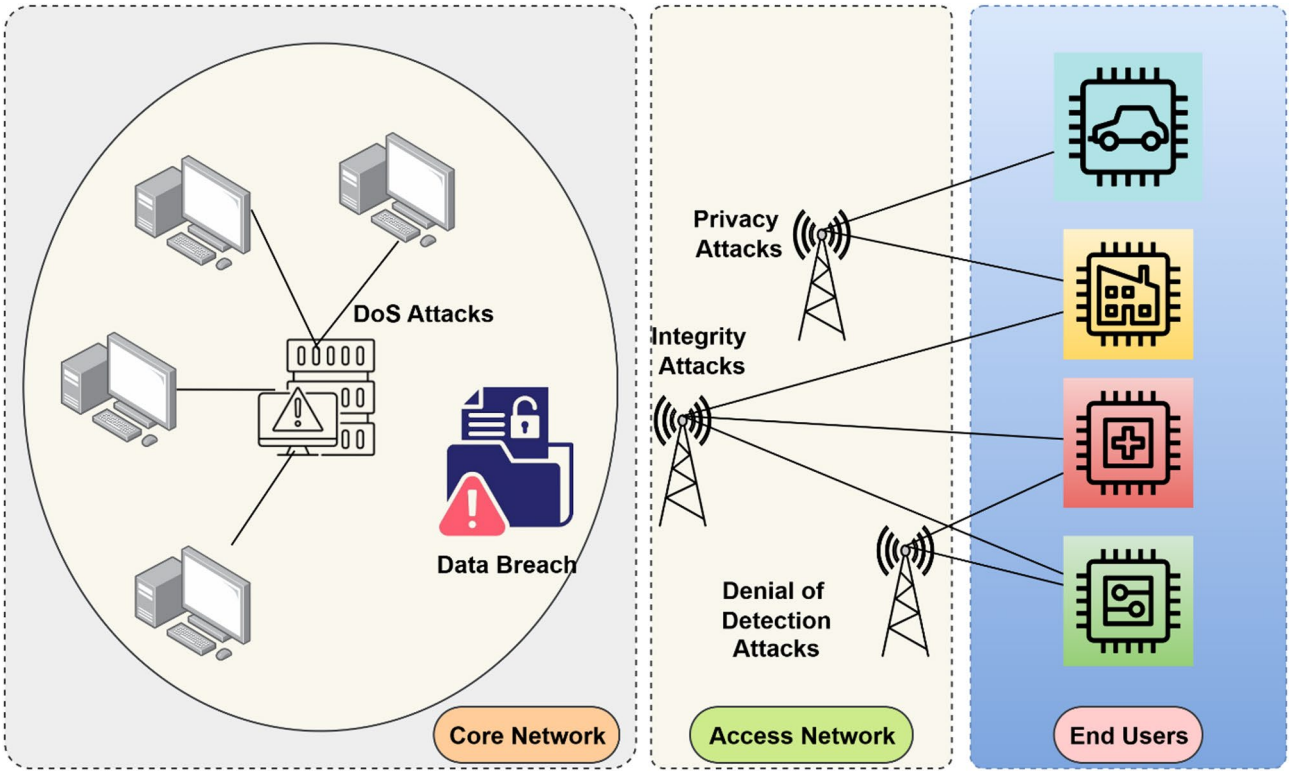

Fig. 1. System model for the Cognitive 5G Network Malicious Users.

Related work

To detect malicious users in collaborative spectrum sensing in cognitive radio network, this paper employed the Extreme Learning Machine (ELM)[16]. The ELM technique was implemented to differentiate between the malicious and the legitimate sensing data due to its fast-training capabilities and great generalization. The ELM model performed better in comparison to a more sophisticated classifier such as SVM, or Decision Trees (DTs), in identifying attempts of falsification of spectrum sensing with high accuracy of detection and low False Alarm Rates (FARs). Free access of the clean labelled information was imperative to the success of the method. It also failed to adapt to rapidly changing network environments real time and was also prone to malicious inputs.

The study proposed, in the context of assessing as well as categorizing risks in 5 g cognitive radio systems, an ensemble method of deep learning, involved the combination of numerous neural networks[17]. The ensemble methodology applied a range of structures to become more robust. The ensemble method greatly enhanced the precision associated with the threat detection where the overlap effect as well as the covert or concealed attacks were also observed. Its high complexity of processing and inference latency were its main constraints and finding edge devices, or mobile ones were complicated to apply in real-time without additional optimization.

The work in[18] used an approach to deep learning to detect encrypted traffic by using AI to detect any ill aims in encrypted 5G networks data streams. It applied flow-oriented features as opposed to payload content. The method aided in providing security to sharing information in 5G networks without compromising the integrity of encryption as it is effective in detecting and identifying different types of malicious encrypted traffic. One may need to retrain the technique often to adjust to changeable traffic patterns and the technique may face challenges by zero-day attacks. Also, in a few cases, it may occur that it could cause ambiguous classification, where some extracted characteristics were described by the encrypted flows.

A Self-Attention Recurrent Neural Network Autoencoder (RNN-AE) can be applied to real-time spectral intrusion detection[19]. Although the AE design separated anomalies, the self-attention process accelerated information gathering of the time context. Tiny spectral activity invasions were detected very well and only a few false positives were obtained. Furthermore, it showed good real time capabilities in detection of spectral anomalies. The technique had performed well in the case of detection, but it may be computationally very demanding on the continuous spectrum monitoring. Additionally, the quality of its effectiveness was also spoiled by the noise training information and by the uncalibration of thresholds that took place during the reconstruction process.

To study the changing malicious traffics trend in 5G, this literature developed intrusion detection based on incremental learning[20]. To dynamically learn new ways of detection, it introduced the concept of machine learning and real-time traffic monitoring. The learning-incremental approach also contributed to greater use and a massive decrease in deterioration of the model over time because of the flexibility of the method related to the new attacks. The updates can come in the form of incremental updates, which can introduce inaccurate

or harmful information and at the same time add flexibility. Training was insufficient, thus creating the danger of catastrophic lapse.

In order to safeguard CR-IoT networks, the study proposes OntoBlock, a platform that combined blockchain-augmented spectrum sensing with ontology-driven threat modelling[21]. It blended trust validation with semantic reasoning. Using blockchain information, ontological danger patterns, as well as spectrum sensing reports, OntoBlock effectively detected and halted malicious user behavior. It made traceability possible as well as increased confidence. When ontologies as well as blockchain were used together, system complexity and latency increase. To function effectively, it required well-defined ontological methodologies as well as a wealth of available resources. Some of the features and challenges of traditional models are given in Table 1.

Problem statement

Although the goal of cognitive 5G networks is to effectively utilize underutilized spectrum, their dynamic as well as decentralized nature makes them susceptible to security threats, particularly from malicious users. These adversaries can carry out attacks such as main user simulation, jamming, as well as spectrum sensing data modification, which can lower network effectiveness, disrupt communication, and Denial of Service (DoS) for authorized users. Existing detection techniques usually rely on inflexible rule-oriented frameworks or conventional machine learning methods, which lack the adaptability as well as accuracy needed to function effectively in the quickly evolving 5G environment. Furthermore, their limited scalability as well as high FPRs hinder their usefulness. Accurately identifying malicious users in cognitive 5G networks beneath a variety of operational situations as well as traffic patterns requires a robust and efficient classification framework. Developing a reliable system that ensures safe spectrum access, lowers the likelihood of misclassification, as well as maintains network effectiveness and confidence describes the problem.

Proposed methodology

Proposed model

The proposed MUC-C5GN model is composed of various phases such as data collection, pre-processing, feature extraction and classification. The initial data is obtained from 5G-NIDD, a typical benchmark source. The gathered data is processed using the normalization as well as scaling procedures. The Self-Attention RNN-AE technique is then used to extract features from the previously processed data. Finally, in cognitive 5G networks, the novel IBERT model performs the categorization of malicious users. ROA, an optimization technique inspired by nature, is used to modify the parameters of BERT. For the entire MUC-C5GN model, the objective function is thought to be maximizing accuracy. This proposed IBERT-ROA of the MUC-C5GN model classifies the final output into seven classes such as normal, User Datagram Protocol (UDP), HyperText Transfer Protocol Flood (HTTP) Flood, port-scan attacks, Internet Control Message Protocol (ICMP), Synchronize (SYN) and Slow rate respectively. The overall proposed MUC-C5GN model is displayed diagrammatically in Fig. 2.

Dataset description

A big, useful dataset called the 5G-NIDD is developed to evaluate techniques for identifying malicious users in 5G network environments. It was taken from a real-world 5G test environment and includes a variety of traffic kinds, involving regular communication as well as a number of attack techniques, including UDP flood,

Citation	Methodology	Features	Challenges
[22]	Machine learning models	Fast as well as adaptive threat detection	Needs frequent retraining
[23]	Reputation-based fusion algorithm	Robust against data falsification	Slower convergence
[24]	Federated learning	Minimizes requirement for central data storage	High communication overhead
[25]	Deep learning	Improved sensing accuracy	Hardware deployment complexity
[26]	Hybrid model combining GRU and SVM	Enhances detection accuracy over standalone methods	Needs optimal hyper parameter tuning
[27]	Behavioral as well as slicing-oriented anomaly detection	Performs better in virtualized 5G environments	Detection may lag real-time events
[28]	DeepTransIDS	Efficient even with class imbalance	Feasibly higher computational cost than simpler methods
[29]	contrastive learning	Offers visualization for interpretability.	Potential high computational needs for training
[30]	Transformer model	Handles data efficiently.	Complexity of overfitting
[31]	Zero-shot prompting	Minimizes manual analysis time	Certain detected vulnerabilities remain unverified.
[32]	LSTM	Scalable and applicable for real-time IoT contexts.	Needs substantial training resources.
[33]	ML/DL models	Improves interpretability as well as analyst trust in AI-driven detection	Ongoing problems with class imbalance
[34]	Transformer-based neural network	Adapts to local traffic changes for enhanced effectiveness.	Needs stable communication for federated modifications
[35]	Federated learning	Adaptable to distinct deployment scenarios.	Needs important computation at edge nodes
[36]	Auditor-oriented verification tree	Eradicates transitive trust dependency, describing collusion attacks	Includes latency in verification.
[37]	Self-Supervised Learning (SSL)	Scalable to vast automotive frameworks	Potential complexity in deployment across heterogeneous vehicle frameworks.

Table 1. Features and challenges of traditional models.

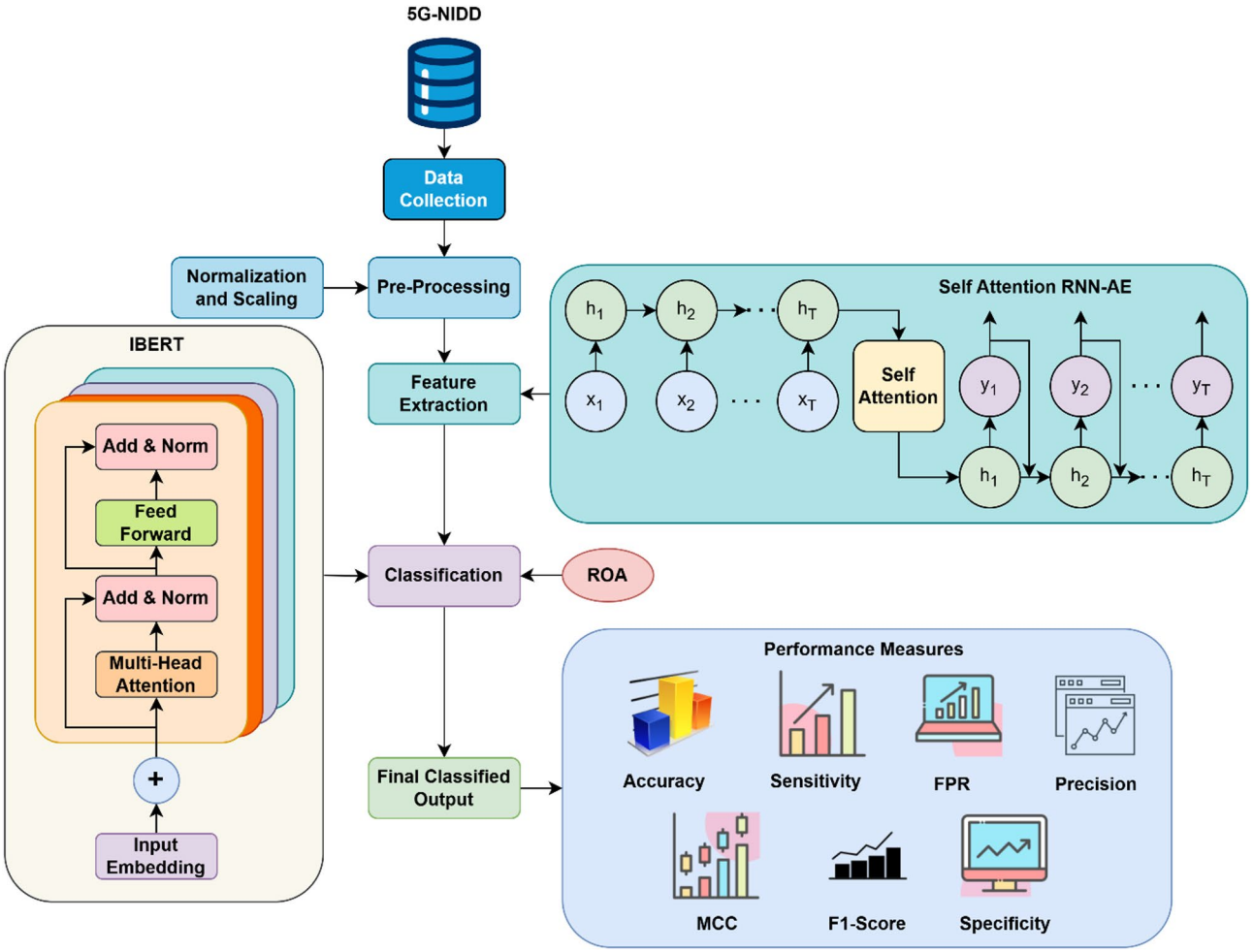

Fig. 2. Overall Proposed MUC-C5GN model.

ICMP flood, HTTP flood, SYN flood and port-scan attacks. The dataset allows for both flow-oriented as well as packet-level analysis since it contains traffic logs in formats including CSV, pcapng, and Argus. To facilitate supervised machine learning tasks, each sample is labelled to distinguish among benign and harmful activity. Because it replicates real traffic contexts across multiple network interfaces, 5G-NIDD is especially helpful for researching cognitive 5G networks. It facilitates the development as well as validation of classification methods that can identify malicious secondary users or anomalous behaviors in situations involving fluctuating spectrum access. Because of its architecture, it may be used to train, test, as well as assess classification algorithms in both federated and centralized intrusion detection frameworks.

An actual 5G testbed (the 5GTN in Oulu, Finland) is used to build the fully annotated 5G-NIDD dataset, which documents network traffic flows under both typical use as well as a variety of attack scenarios. Approximately 1,215,890 network flow records in total. A vector of 112 input attributes, including data from several network levels (IP, TCP/UDP, and application—like HTTP, HTTPS, SSH, and SFTP), is used to represent each flow. Network metrics are mostly flow-oriented (Layer 3/4 information after GTP removal). It shows combination of higher-level indications like HTTP/SSH/SFTP trends with protocol-specific characteristics (such as packet and byte counts, time intervals, as well as indicators) within IP, TCP, UDP, and ICMP. Class ratios are maintained by stratified divisions (e.g., 80% for training and 20% for testing), which is crucial given the class imbalance (e.g., ICMP Flood is notably under-described relative to UDP Flood). The class distribution by the count of flows is shown in Table 2.

Pre-processing by normalization and scaling

In cognitive 5G networks, pre-processing is crucial for increasing the accuracy as well as efficacy related to malicious user categorization. Efficient pre-processing is crucial to ensuring that the input for classification methods is consistent, important, as well as unambiguous due to the high amount, diversity, as well as noise in raw network traffic information. In the dynamic, spectrum-sharing scenarios typical of cognitive 5G networks, the various pre-processing steps are essential for improving model generalization, reducing false positives, as well as enabling real-time detection of malicious users.

Class	Number of flows
Benign	477,737
HTTP Flood	140,812
ICMP Flood	1,155
SYN Flood	9,721
SYN Scan	20,043
Slowrate DoS	73,124
TCP Connect Scan	20,052
UDP Flood	457,340
UDP Scan	15,906

Table 2. Class distribution by the number of Flows.

In cognitive 5G networks, normalization as well as scaling are crucial pre-processing techniques for getting network traffic information ready for malicious user classification. Directly feeding raw network traffic data (like signal strength, inter-arrival time, packet size, as well as port numbers) into a machine learning model might lead to biased results since they vary in scale and unit. Normalization is essential to ensure that every feature has an equal influence on the final choice since machine learning methods are extremely sensitive to the size of features.

Min-Max Normalization describes a commonly used technique that modifies the data to fit inside a given range, often [0, 1]. This is particularly advantageous when the method assumes that the input characteristics are distributed consistently. The formula is:

$$y' = \frac{y - y_{Min}}{y_{Max} - y_{Min}} \tag{1}$$

Here, the normalized feature value is shown by y', minimum as well as maximum values of that feature is shown by y_{Min} and y_{Max} and the original feature value is given by y respectively.

Z-score Normalization (Standardization) describes a frequently used technique that modifies the feature values to have a variance of one as well as a mean of zero. This is particularly helpful when traits have a Gaussian distribution. The formula is:

$$y' = \frac{y - \mu}{\sigma} \tag{2}$$

Here, the standardized feature is shown by y', standard deviation is shown by σ and the mean associated with the feature is shown by μ respectively.

The process of normalization enhances the effectiveness of the training process and convergence of the machine learning approaches in the cognitive 5G scenarios where the properties to be learned are of significantly different scales, e.g., Signal-to-Noise Ratio (SNR) is calculated in decibels and packet sizes are value in bytes in the 5G-NIDD dataset. Moreover, it minimizes the effect of significant features alongside increasing the capacity of a classifier to identify the slightest changes caused by malicious users, e.g. aberrant timing schemes or spastic transmission rates. Thus, in medium to large, real-time 5G network scenarios, normalization is workable along with scaling enhancement model effectiveness, less amount of false positive, as well as general detection trust.

Feature extraction by Self-Attention RNN-AE

In the cognitive 5G networks, feature extraction is the important component in the characterization of malicious users since it creates clear and understandable descriptions of raw network data that is deemed suitable in machine learning algorithms. Efficient feature extraction makes it possible to determine the main behavioral qualities that can serve as the criteria of distinguishing fraudulent user and legal users in high-dimensional, dynamic 5G environments. Spectrum data or traffic logs can all be used to extract statistical features (e.g. signal strength change, average packet size), temporal features (e.g. session length, time between arrivals), and protocol-specific measures (e.g. number of flags, port access frequency). With cognitive 5G networks, where malicious users tend to disguise themselves as regular communicators, feature extraction minimizes requirements on processing, enhances accuracy of classifications, and also facilitates quicker and real-time detection of abnormalities by focusing on key attributes.

Self-Attention RNN-AE is an effective feature extraction utility which is capable of learning both temporal and contextual relationships in sequential network traffic streams, which is valuable as far as detection of malicious users in cognitive 5G networks is concerned. Malicious actions like false spectrum sensing or jamming messages in cognitive 5G networks tend to be not only subtle but also temporally and spatially diffused and are high dimensional. Self-attention RNN-AEs are especially useful since identifying such complex patterns may be tricky by using conventional feature extraction.

The two primary components of an RNN-AE are a decoder RNN that reconstructs the original sequence using the encoded features as well as an encoder RNN that compresses input sequences into a latent feature description. The encoder calculates hidden states i_u for each time step u of an input sequence $Y = \{y_1, y_2, \cdots, y_U\}$in a mathematical format as follows:

$$i_u = g\left(i_{u-1}, y_u\right) \tag{3}$$

Here, g describes a recurrent function like GRU or LSTM. The encoded latent vector a is generally derived from the final hidden state i_U as follows.

$$a = i_U \tag{4}$$

The decoder next plans to reconstruct the sequence $\widehat{Y} = \{\widehat{y}_1, \widehat{y}_2, \cdots, \widehat{y}_U\}$ utilizing:

$$\widehat{y}_u = h\left(i'_u\right), \quad i'_u = g\left(i'_{u-1}, \widehat{y}_{u-1}\right) \tag{5}$$

The reconstruction error is intended to be decreased by the method:

$$M_{Rec} = \sum\nolimits_{u=1}^{U} \| y_u - \widehat{y}_u \|^2 \tag{6}$$

A self-attention procedure is included to enhance the method's ability to focus on important parts related to the sequence. Varied time steps are given varied weights by the attention procedure based on how important they are. For a hidden state matrix $I = [i_1, i_2, \cdots, i_U]$, attention weights α_u are measured as below.

$$\alpha_u = \frac{exp\left(f_u\right)}{\sum_{l=1}^{U} exp\left(f_l\right)}, \quad f_u = score\left(i_u\right) \tag{7}$$

Either a trainable feedforward layer or the dot product are common scoring functions. Next, a weighted total is produced for the context vector d:

$$d = \sum\nolimits_{u=1}^{U} \alpha_u i_u \tag{8}$$

The last extracted feature, represented by the context vector d, captures both temporal dependencies as well as notable patterns that are critical for identifying malicious activity. These identified properties enable the classifiers of cognitive 5G networks to dissimilarity between adversaries involved in covert attacks such as Spectrum Sensing Data Falsification (SSDF) besides Primary User Emulation (PUE) and licensed users. In the noisiest or partly observed domains, immense precision plus endurance is attained upon using sequence learning of RNN and dynamic the focus capacity of attention. The Self-Attention RNN-AE has become one of the leading techniques of feature extraction in intelligent spectrum access schemes (as well as safe) via 5G cognitive radio systems.

Classification by novel IBERT

Classification in cognitive 5G networks is very significant in recognizing malicious users, where illicit or fraudulent actions of an impersonator, jammers or misusers of spectrum sensing data can be automatically identified. When relevant features have been extracted in the network traffic or signal or it is done in the signal data, classification algorithms are applied to determine the user as malicious or not. These classifiers analyze labelled datasets to determine a pattern that suggests abnormal activities so that there is the possibility of both fast and correct identification of threats in variable and fast-dynamically changing 5G environments. Both efficiency and safety of cognitive 5G systems are based on effective segregation, which also guarantees maximum utilization of the spectrum, safeguards the dependability of communication, and maintains the integrity pertaining to the dynamic spectrum access.

The capability of BERT to understand complex contextual relationships in sequential data has lots of benefits in terms of malicious users' classification in cognitive 5G networks. BERT has been especially successful at studying both time-based and protocol-level trends of network traffice since, unlike existing approaches whose analysis is restricted to one direction i.e., both past and future effects are unknown, it employs a bi-directional attention process to discern their previous and future dependencies. This is how BERT is able to detect minor anomalies capable of signifying the existence of dangerous behaviour, including data tampering or spectrum abuse. It can be well generalized with access to limited labelled data even though the data is only labelled as 5G, as its pre-training has enough large datasets.

Moreover, BERT can be tuned to be efficient to numerous classification tasks with minimum adjustment to its structure. These properties lead to higher detection rates, lower false alarms and high reliability in action in complex and dynamic area that define the cognitive 5G networks. BERT has numerous drawbacks that negate BERT benefits even though it can be well used in the case of malicious user categorization in cognitive 5G networks. It is very complex, computationally and very resource-demanding. Because of its high memory and processing needs, BERT cannot be as easily applied to real-time usage in edge, or otherwise resource-limited devices in a network, particularly in a 5G network. Additionally, it might take quite some time to fine-tune or tweak it into becoming as effective as possible in cybersecurity tasks because the organization of network traffic is not necessarily going to gel perfectly with the linguistic information that it initially trained on. Due to the fact that BERT approaches are often difficult to interpret or obscure, they challenge issues of not only explainability but also trust in security-sensitive systems.

Moreover, when there is insufficient labelled information specific to the domain, BERT can either overfit or perform poorly with malicious activity being rare or when the dataset is significantly imbalanced. These issues

constrain the BERT applicability in certain hostile user identification that are real time or run on lightweighted hosts in cognitive 5G networks. The new IBERT has numerous benefits in terms of classifying malicious users in the cognitive 5G networks by enhancing the efficiency and the versatility of the original BERT design. IBERT is far better suited to real-time edge inference using limited-capable devices, a typical 5G scenario, after its enhanced version that provides integer quantization, a lower attention computational complexity, and a simplified model compression. While drastically reducing latency as well as memory usage, it maintains the robust contextual comprehension of regular BERT, enabling faster detection of malicious activities such as spoofing, jamming, or spectrum sensing manipulation. Furthermore, IBERT can more successfully adapt to domain-specific traffic anomalies as well as behaviors while preserving classification accuracy thanks to its improved fine-tuning capability. With these advantages, IBERT is positioned as a strong choice for high-performance, deployable, as well as scalable malicious user detection in the dynamic, dispersed environment of cognitive 5G networks.

A context-sensitive as well as effective machine learning methodology for MUC-C5GN applications is provided by the IBERT model. Despite its ability to comprehend intricate contextual meanings, classic BERT is resource-intensive as well as difficult to implement in real-time 5G network environments. Using model compression techniques such as integer quantization, weight pruning, as well as attention simplification, IBERT overcomes these difficulties and achieves excellent accuracy having significantly lower memory and processing requirements, making it ideal for deployment at edge or fog nodes within a 5G cognitive paradigm.

IBERT uses just integer arithmetic instead of floating-point computations, while maintaining the Transformer-oriented encoder architecture of BERT. An organized representation of network traffic or user behavior sequences (such as protocol interactions, time patterns, or port use) makes up the input for IBERT. Every input sequence $Y = \{y_1, y_2, \cdots, y_o\}$ is initially embedded as below.

$$F = embedding\ (y_1, y_2, \cdots, y_o) \tag{9}$$

Here, the embedding dimension is shown by e and the input embeddings are shown by $F \in S^{o \times e}$. The attention scores are computed in standard BERT utilizing the following:

$$attention\,(R, L, W) = softmax\left(\frac{RL^T}{\sqrt{e_l}}\right)W \tag{10}$$

In IBERT, this is tuned by quantizing the matrices R, L, W for lowering precision integers in order to enable effective calculation.

$$quantized\ attention\ \ (R, L, W) = softmax\ \left(\frac{R^{(Int)}L^{(Int)T}}{\sqrt{e_l}}\right)W^{(Int)} \tag{11}$$

These quantized procedures significantly reduce the amount of time as well as energy required for inference, which is crucial in 5G edge scenarios. The input description is obtained by pooling the contextual output from the final encoder layer, often using the [CLS] token:

$$a = layer\ norm\ \left(I_{[CLS]}\right) \tag{12}$$

Here, the hidden state respective to the [CLS] token is shown by $I_{[CLS]} \in S^e$. This is transferred via a simple fully connected classifier.

$$\widehat{z} = softmax\ (Xa + c) \tag{13}$$

Here, $X \in S^{d \times e}$, $c \in S^d$ and the count of classes (benign or malicious user) is shown by d. The purpose of the model is to lower the cross-entropy loss:

$$M = -\sum\nolimits_{j=1}^{d} z_j \log\left(\widehat{z}_j\right) \tag{14}$$

Because of its scalability to handle large traffic volumes, excellent accuracy with unbalanced data, as well as real-time inference capabilities, IBERT stands out in cognitive 5G networks. The contextual nature related to the transformer makes it possible to detect minor abnormalities such as PUE and SSDF by recognizing both short- as well as long-range relationships in user behavior. Its lightweight design also makes it easy to integrate with edge devices used for real-time threat detection as well as distributed spectrum monitoring in 5G network slicing. By utilizing contextual sequence modelling in conjunction with low-latency, resource-efficient inference, IBERT provides a robust as well as effective classification method for identifying malicious users in cognitive 5G networks, establishing it as a promising option for secure wireless communication in next generations. The block diagram of novel IBERT for the MUC-C5GN model is displayed in Fig. 3.

ROA algorithm

Optimization is crucial for enhancing the effectiveness of malicious user categorization systems in cognitive 5G networks by modifying model parameters and system resources. This enables more greater accurateness, faster identification, and less False Positive Rates (FPRs). In such complex and dynamic scenarios, optimization methods are employed to change hyperparameters of machine learning models and also achieve a nice balance between sensitivity and specificity of detection. Moreover, optimization enables real-time execution on edge

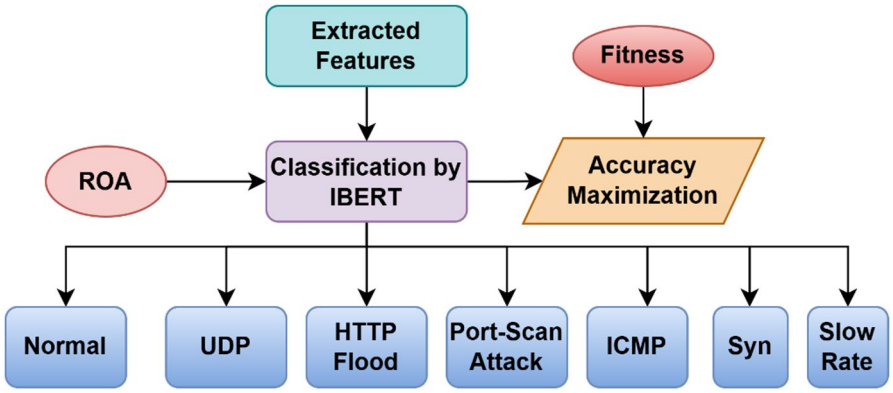

Fig. 3. Block diagram of Novel IBERT for the MUC-C5GN model.

gadgets with scarce resources since it changes the computational intricacy. Optimization also provides accurate and effective threat detection within the spectrum sharing system of cognitive 5G networks due to better model generalization and a reduction in false positive rates in which the non-malicious user is classified as being malicious.

Inspired by social revolutions, ROA divides its methodology into three phases: (i) revolutionary ideology, which lays the foundation for variation; (ii) revolutionary action, which represents metamorphosis; as well as (iii) increased self-awareness, which denotes improvement and adaptability. Each step contributes to a strong mathematical foundation that guides the algorithm's operations.

Because ROA is a population-driven algorithm, it uses a collection of possible solutions to look into the issue. Each solution corresponds to a unique set of decision factors and is represented by a person in the population. Together, these elements make up the solution matrix, which is expressed as mathematical vectors Eq. (15). To ensure sufficient variety as well as prevent early convergence, the starting population is generated at random over the solution space at the start of the process utilizing Eq. (16).

$$Y = \begin{bmatrix} y_{1,1} & \cdots & y_{1,k} & \cdots & y_{1,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ y_{j,1} & \cdots & y_{j,k} & \cdots & y_{j,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ y_{O,1} & \cdots & y_{O,k} & \cdots & y_{O,n} \end{bmatrix}_{O\times n} \tag{15}$$

$$y_{j,k} = LB_k + s \times (UB_k - LB_k) \tag{16}$$

The population matrix is represented by Y in these calculations, the j^{th} member associated with the ROA is indicated by Y_j, the value assigned to the k^{th} variable by the j^{th} member is represented by $y_{j,k}$, and the number of population members as well as problem variables are indicated by O and n, respectively. Every variable's lower as well as upper bounds are represented by the parameters LB_k and UB_k, whereas s describes a random number between 0 and 1.

Following initialization, each member's fitness function is evaluated, producing an aligned vector of function values (Eq. (17)). The current leader, who guides subsequent search stages, describes the person who offers the optimal fitness value.

$$G = \begin{bmatrix} G_1 \\ \vdots \\ G_j \\ \vdots \\ G_O \end{bmatrix}_{O\times 1} = \begin{bmatrix} G(Y_1) \\ \vdots \\ G(Y_j) \\ \vdots \\ G(Y_O) \end{bmatrix}_{O\times 1} \tag{17}$$

Here, the vector related to the fitness function, which includes the general goals associated with the optimization problem, is represented by the symbol G. This vector is increased by each component of the ROA, in which G_j stands for the specific fitness function value associated with the j^{th} member of the ROA.

Three interrelated stages—Revolutionary Ideology, Revolution Movement, as well as Enhancement of Self-awareness—are used by the ROA algorithm to repeatedly alter its population. These phases illustrate the dynamics of revolutions by striking a balance between exploitation (improving existing solutions) and exploration (exploring novel regions).

The population members' placements inside the search space are altered by the leader's beliefs in each ROA iteration. The formula given in Eq. (18) determines a novel position for every individual by taking into account the leader's growing ideological influence. As the algorithm advances, this formula ensures that individuals

gradually come into line with the leader's vision. The update is approved, replacing the individual's previous location as shown in Eq. (19), if the fitness function's value rises with the novel location.

$$y_{j,k}^{Q1} = \left(1 - \frac{u}{U}\right) \cdot\ y_{j,k} + \left(\frac{u}{U}\right) \cdot\ M_k \tag{18}$$

$$Y_j = \begin{cases} Y_j^{Q1}, & G_j^{Q1} < G_j \\ Y_j, & otherwise \end{cases} \tag{19}$$

Here, Y_j^{Q1} represents the updated position related to the j^{th} member of the population in the first stage, whereas $y_{j,k}^{Q1}$ represents the k^{th} component of that updated position. G_j^{Q1} represents the value linked with the fitness function at this novel point. The pioneering leader, represented by M, holds a position with M_k as its k^{th} component. The present iteration is denoted by the variable u, while the total number of iterations allowed by the algorithm is denoted by U. Participants become nearer to the leader's position as iterations go, simulating the increasing alignment of followers with a compelling revolutionary vision over time.

Following the leader's plan determines each individual's starting location in order to mimic the revolutionary movement stage in ROA. Equation (20), which shows how individuals alter their behaviors to fit the leader's influence, is used to achieve this. The calculated shifts show notable changes in the individual's positions, promoting global investigation in different regions related to the search space. Finding better solutions is more likely as a result of this thorough examination. If the updated location improves the fitness function's result, as shown in Eq. (21), it is maintained.

$$y_{j,k}^{Q2} = y_{j,k}^{Q2} + s \cdot\ \left(M_k - J \cdot\ y_{j,k}^{Q2}\right) \tag{20}$$

$$Y_j = \begin{cases} Y_j^{Q2}, & G_j^{Q2} < G_j \\ Y_j, & otherwise \end{cases} \tag{21}$$

In this case, the newly calculated position for the j^{th} population individual in the second stage of ROA is denoted by Y_j^{Q2}, and the k^{th} dimension of this position is denoted by $y_{j,k}^{Q2}$. Here, G_j^{Q2} represents the value associated with the fitness function. The leader's location is indicated by the symbol M, and the k^{th} element of that location is represented by M_k. Randomness is added to the alteration by selecting the variable J at random from the collection {1,2}. Additionally, s describes a random value between 0 and 1, which adds unpredictability to ensure a variety of investigation.

The program randomly generates a novel place near every population individual's existing position in order to replicate the third stage of ROA. This approach demonstrates the little changes people make as a result of reflection and learning. Equation (22) was used to calculate these little locational modifications, which are intended to assist the individuals in gradually improving their solutions. These small-scale modifications ensure that the search prioritizes using local areas of the issue space, which improves the algorithm's capacity to find better solutions close to those that have previously been discovered. The goal of the modification procedure is to increase the search's precision, which complements the broader analysis carried out in earlier phases.

As shown in Eq. (23), every individual's updated location will only be approved if it results in a higher fitness function value. This approach ensures that the algorithm keeps beneficial changes while removing ineffective ones.

$$y_{j,k}^{Q3} = \begin{cases} y_{j,k} + s\left(y_{j,k}^{OLD} - y_{j,k}\right), & G_j^{OLD} < G_j \\ y_{j,k} + s\left(y_{j,k} - y_{j,k}^{OLD}\right), & otherwise \end{cases} \tag{22}$$

$$Y_j = \begin{cases} Y_j^{Q3}, & G_j^{Q3} < G_j \\ Y_j, & otherwise \end{cases} \tag{23}$$

Here, Y_j^{Q3} denotes the j^{th} individual's freshly established location in the third stage of ROA, whereas $y_{j,k}^{Q3}$ refers to its k^{th} dimension. The fitness function value at the updated location is represented by the value G_j^{Q3}. The k^{th} dimension associated with the individual's location from the earlier iteration (i.e., $u-1$) is indicated by the symbol $y_{j,k}^{OLD}$, and the fitness function value at that earlier location is shown by G_j^{OLD}. The pseudocode of ROA is displayed in Algorithm 1 and the flow model of ROA for the MUC-C5GN model is shown in Fig. 4.

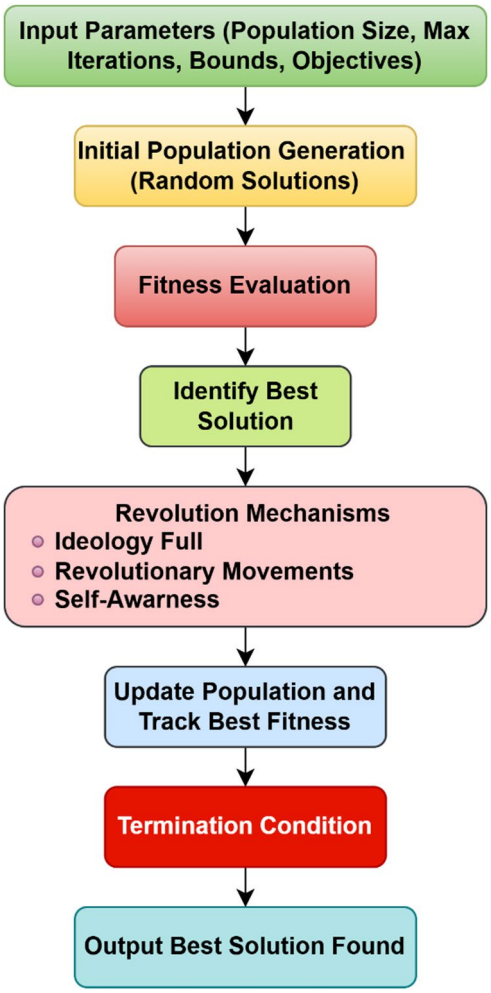

Fig. 4. Flow model of ROA for the MUC-C5GN model.

Start

Input dimension, population size, maximum iterations, lower bound and upper bound [extracted features of the proposed MUC-C5GN model]

Output best solution attained [maximized accuracy of the proposed MUC-C5GN model]

$$y_{j,k} = LB_k + s \times (UB_k - LB_k)$$

$$G = \begin{bmatrix} G_1 \\ \vdots \\ G_j \\ \vdots \\ G_O \end{bmatrix}_{O\times 1} = \begin{bmatrix} G(Y_1) \\ \vdots \\ G(Y_j) \\ \vdots \\ G(Y_O) \end{bmatrix}_{O\times 1}$$

Identify leader with minimum G

For $u = 1$ *to* U *do*

For every individual j *in population [Phase 1]*

For every variable k

$$y_{j,k}^{Q1} = \left(1 - \frac{u}{U}\right) \cdot y_{j,k} + \left(\frac{u}{U}\right) \cdot M_k$$

$$Y_j = \begin{cases} Y_j^{Q1}, & G_j^{Q1} < G_j \\ Y_j, & otherwise \end{cases}$$

For every individual j *in population [Phase 2]*

$J =$ *random selection from* $\{1,2\}$

For every variable k

$$y_{j,k}^{Q2} = y_{j,k}^{Q2} + s \cdot \left(M_k - J \cdot y_{j,k}^{Q2}\right)$$

$$Y_j = \begin{cases} Y_j^{Q2}, & G_j^{Q2} < G_j \\ Y_j, & otherwise \end{cases}$$

For every individual j *in population [Phase 3]*

For every variable k

If $G_j^{OLD} < G_j$

$$y_{j,k} + s\left(y_{j,k}^{OLD} - y_{j,k}\right)$$

else

$$y_{j,k} + s\left(y_{j,k} - y_{j,k}^{OLD}\right)$$

$$Y_j = \begin{cases} Y_j^{Q3}, & G_j^{Q3} < G_j \\ Y_j, & otherwise \end{cases}$$

Update leader if better solution is attained

Return leader (optimal solution) [maximized accuracy value of the proposed MUC-C5GN model]

Stop

Algorithm 1 ROA

Results and analysis

Experimental setup

The proposed IBERT-ROA for the MUC-C5GN model was implemented in MATLAB and the findings were discussed. The population size and the iteration count was taken to be 10 and 200. The proposed IBERT-ROA was compared with numerous models like LSTM-GRU, MLP, Chaotic DBN and Detectron2 + YOLOv7 with

consideration of analysis such as accuracy, sensitivity, FPR, precision, Matthews Correlation Coefficient (MCC), F1 Score and specificity to reveal the superiority of the proposed MUC-C5GN model.

Accuracy analysis

The MUC-C5GN accuracy evaluation demonstrates the proposed IBERT-ROA model's exceptional as well as reliable effectiveness throughout 200 iterations as in Fig. 5. With a starting classification accuracy of 92.49% at 20 iterations as well as reaching 99.74% at 200 iterations, IBERT-ROA consistently improves and outperforms entire other approaches. Although their progress seems more slow, Detectron2 + YOLOv7 also obtains outstanding findings, peaking at 98.40%. Chaotic DBN comes in second, at 97.46%. Despite improving over iterations, LSTM-GRU as well as MLP still perform poorly, with ultimate accuracies of 97.08% and 94.91%, respectively. The results show that IBERT-ROA exhibits strong generalization as well as convergence capabilities, maintaining high accuracy from the first iterations while scaling better with further training. This demonstrates that IBERT-ROA describes a very effective method for accurately as well as scalable identifying malicious users in dynamic cognitive 5G network environments. The proposed IBERT-ROA for the MUC-C5GN model in terms of accuracy is 2.74%, 5.09%, 2.34% and 1.36% better than LSTM-GRU, MLP, Chaotic DBN and Detectron2 + YOLOv7 respectively.

Sensitivity analysis

The proposed IBERT-ROA model's improved detection capability across entire iterations is demonstrated by the sensitivity analysis for MUC-C5GN as in Fig. 6. The proposed approach continuously outperforms conventional methods, with a strong sensitivity of 89.41% at 20 iterations as well as gradually improving to 98.48% at 200 iterations. Impressive sensitivity is also demonstrated by Detectron2 + YOLOv7, which ends at 97.17% and is followed by Chaotic DBN at 95.10%. Both show consistent as well as reliable effectiveness. By contrast, LSTM-GRU as well as MLP exhibit reduced sensitivity, attaining 92.91% and 93.08% in the final iteration, respectively. As the number of iterations increases, the sensitivity gradually increases, demonstrating the model's strong

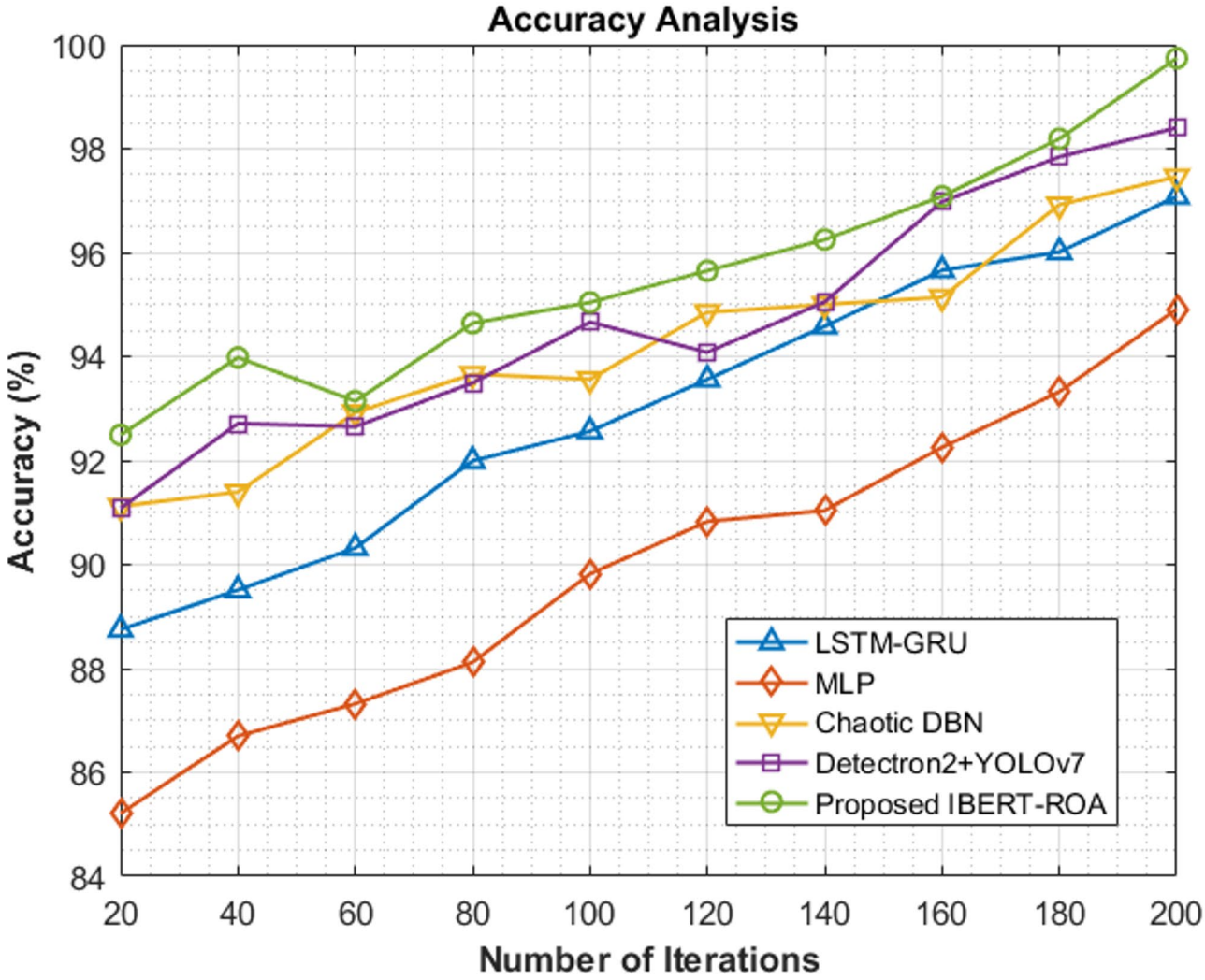

Fig. 5. Accuracy analysis.

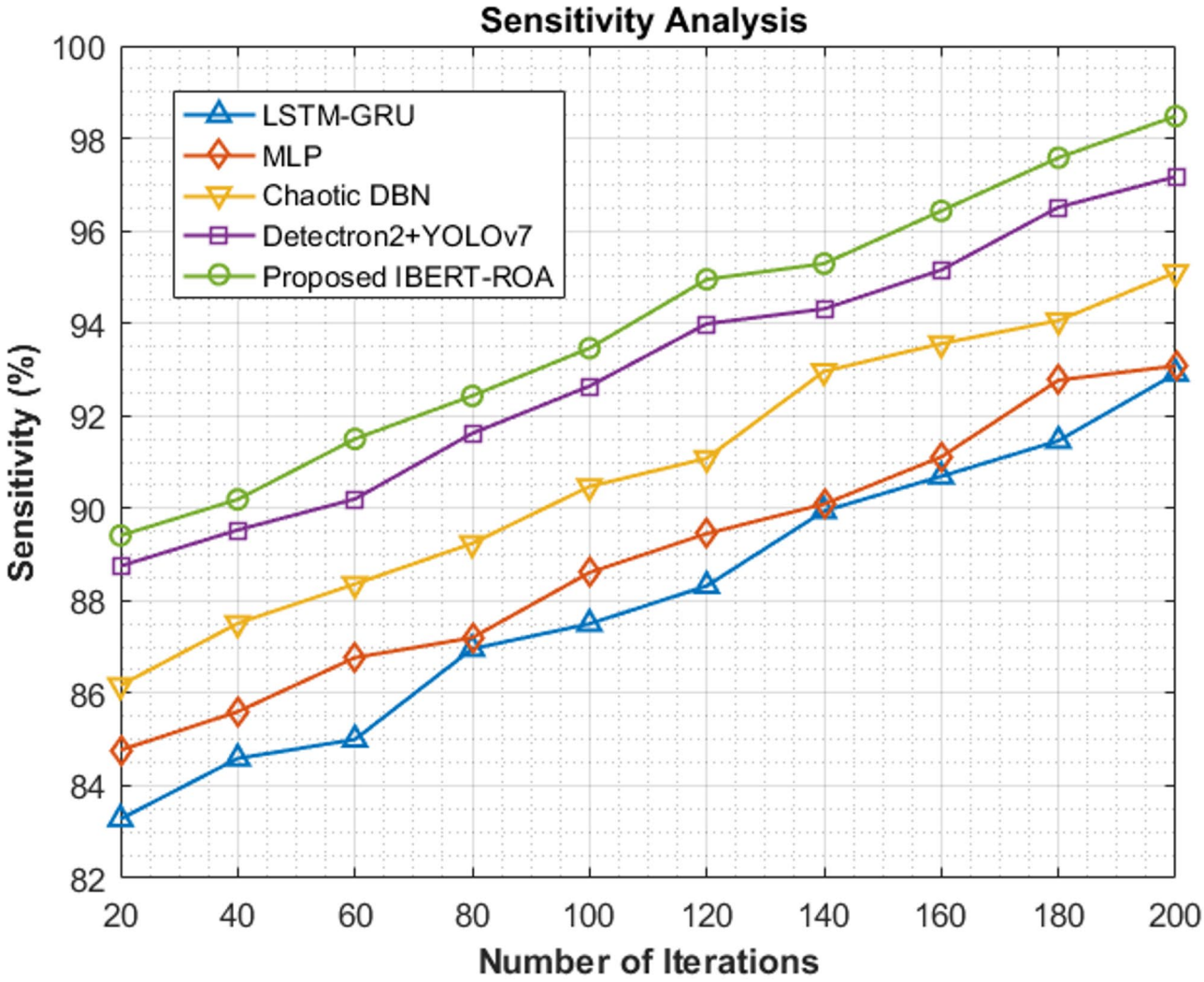

Fig. 6. Sensitivity analysis.

ability to accurately detect real malicious users. This consistent as well as high sensitivity over the training spectrum demonstrates IBERT-ROA's robustness and flexibility in dynamic 5G cognitive environments, in which lowering false negatives is essential to guaranteeing reliable and secure communication. The sensitivity gains of the proposed IBERT-ROA for the MUC-C5GN model over LSTM-GRU, MLP, Chaotic DBN, and Detectron2 + YOLOv7 are 5.99%, 5.80%, 3.55% and 1.35%, respectively.

FPR analysis

The effectiveness of the proposed IBERT-ROA in lowering incorrect categorization of malicious users is highlighted by the FPR study of MUC-C5GN as in Fig. 7. Its remarkable capacity to eliminate false alarms is demonstrated by its steady decline from a low FPR of 3.96% at 20 iterations to an amazing 1.16% by 200 iterations. On the other hand, traditional models like LSTM-GRU as well as Detectron2 + YOLOv7 have noticeably higher FPRs throughout the course of iterations; LSTM-GRU starts at 8.74% and only reaches 2.09%, whilst YOLOv7 exhibits more fluctuation before levelling off. Over time, MLP as well as Chaotic DBN also reduce FPRs, although not as well as IBERT-ROA. The proposed model's continuously lower FPR demonstrates its capacity to maintain high classification accuracy while maintaining sensitivity, which is critical in 5G cognitive networks in which user confidence as well as efficient spectrum usage are critical. For the MUC-C5GN model, the suggested IBERT-ROA outperforms LSTM-GRU, MLP, Chaotic DBN, and Detectron2 + YOLOv7 in terms of FPR by 44.50%, 54.86%, 48.67% and 44.23%, respectively.

Precision analysis

The MUC-C5GN precision study demonstrates the proposed IBERT-ROA's capacity to detect malicious users with fewer false positives as in Fig. 8. From 89.84 to 98.91% by the 200th iteration, IBERT-ROA consistently outperforms entire remaining approaches tested. Despite showing somewhat fewer consistency in the early rounds, Detectron2 + YOLOv7 comes in second with excellent performance, reaching 97.25%. While LSTM-GRU records a lower ultimate precision of 94.10%, MLP as well as Chaotic DBN show progressive increases,

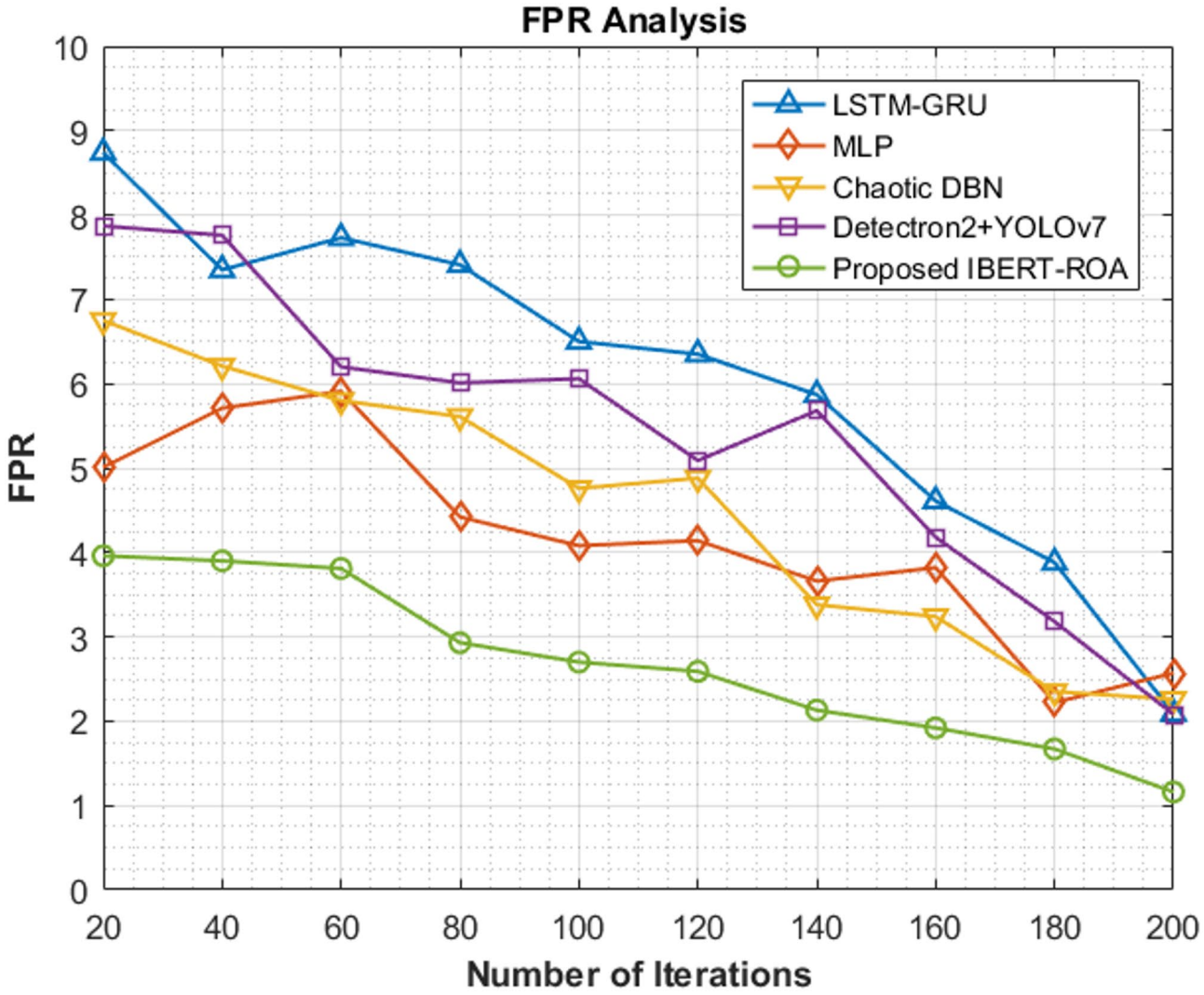

Fig. 7. FPR analysis.

culminating at 96.12% and 95.20% respectively. Strong dependability for threat detection in sensitive cognitive 5G network scenarios is ensured by the notable increase in precision during training iterations for IBERT-ROA, which highlights its capacity to properly detect malicious actions while avoiding misclassifying legitimate users. This remarkable precision shows how well the model learns as well as generalizes in complex, real-time communication networks. The suggested IBERT-ROA outperforms LSTM-GRU, MLP, Chaotic DBN, and Detectron2 + YOLOv7 in terms of precision for the MUC-C5GN model by 5.11%, 2.90%, 3.90% and 1.71%, respectively.

MCC analysis

The proposed IBERT-ROA model's improved prediction accuracy is demonstrated by the MCC analysis for MUC-C5GN as in Fig. 9. IBERT-ROA consistently outperforms entire remaining models in each iteration, starting at 88.45% as well as reaching a peak of 97.82% by the 200th iteration. Because it balances true and false positives as well as negatives, MCC seems to be essential for evaluating models on unbalanced datasets. With MCC ratings of 96.91% and 95.34%, respectively, Chaotic DBN and LSTM-GRU demonstrate strong but slightly inconsistent effectiveness. The final MCC values for MLP as well as Detectron2 + YOLOv7 show moderate increases, at 93.98% and 94.73%. IBERT-ROA's steady as well as high MCC development underpins its dependability, stability, and superior generalization in a variety of scenarios, making it highly efficient for reliable and scalable threat detection in complex cognitive 5G environments. In terms of MCC for the MUC-C5GN model, the suggested IBERT-ROA outperforms LSTM-GRU, MLP, Chaotic DBN, and Detectron2 + YOLOv7 by 2.60%, 4.09%, 0.94% and 3.26%, respectively.

F1 score analysis

The proposed IBERT-ROA model's exceptional performance in achieving a superb balance among precision as well as recall is highlighted by the F1 Score evaluation for MUC-C5GN in Fig. 10. It continuously improves

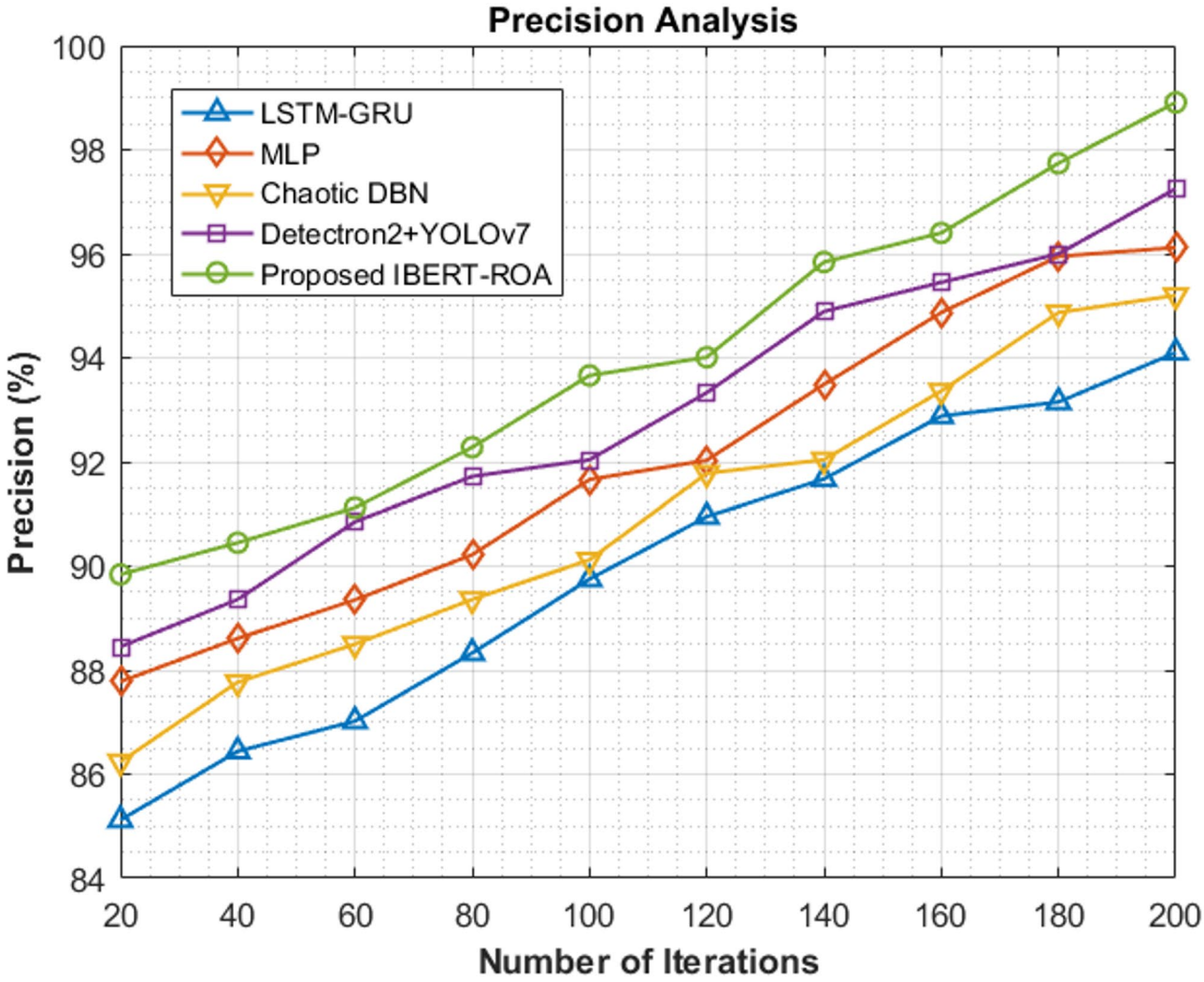

Fig. 8. Precision analysis.

over the iterations, reaching an astounding 98.01% at the 200th iteration after starting with a strong F1 Score of 89.12% at 20 iterations. The model's ability to accurately recognize malicious users while lowering inaccurate classifications is seen by this consistent growth. Comparatively, Detectron2 + YOLOv7 as well as LSTM-GRU accomplish well, attaining final F1 Scores of 96.68% and 97.14%, respectively, although both initial and subsequent iterations fail to meet IBERT-ROA. Both MLP as well as Chaotic DBN accomplish inadequately, peaking at 94.58% and 95.14%. The F1 Score trend clearly illustrates IBERT-ROA's improved capacity to deliver balanced, high-quality classification effectiveness, which is essential for accurate as well as rapid threat detection in cognitive 5G network environments. The suggested IBERT-ROA outperforms LSTM-GRU, MLP, Chaotic DBN, and Detectron2 + YOLOv7 in terms of F1 Score for the MUC-C5GN model by 0.90%, 3.63%, 3.02% and 1.38%, respectively.

Specificity analysis

The proposed IBERT-ROA model's effectiveness in correctly identifying authorized users as well as lowering false positives is demonstrated by the specificity study for MUC-C5GN in Fig. 11. IBERT-ROA consistently outperforms entire remaining models throughout training, achieving 98.91% by the 200th iteration after beginning with a high specificity of 89.88% after 20 iterations. Although they do not equal the findings of the suggested model, Chaotic DBN as well as MLP also exhibit noteworthy specificity, peaking at 97.81% and 96.80%, respectively. Moderate improvements are shown by LSTM-GRU as well as Detectron2 + YOLOv7, which achieve 94.76% and 95.25%, respectively. IBERT-ROA's sophisticated as well as high specificity ratings show how well it can preserve network trust by reducing false alarms. In 5G cognitive systems, where accurate differentiation among benign as well as malicious users ensures safe, efficient spectrum access and network dependability, this feature is particularly crucial. In the specificity for the MUC-C5GN model, the suggested IBERT-ROA outperforms LSTM-GRU, MLP, Chaotic DBN, and Detectron2 + YOLOv7 by 4.38%, 2.18%, 1.12% and 3.84% respectively.

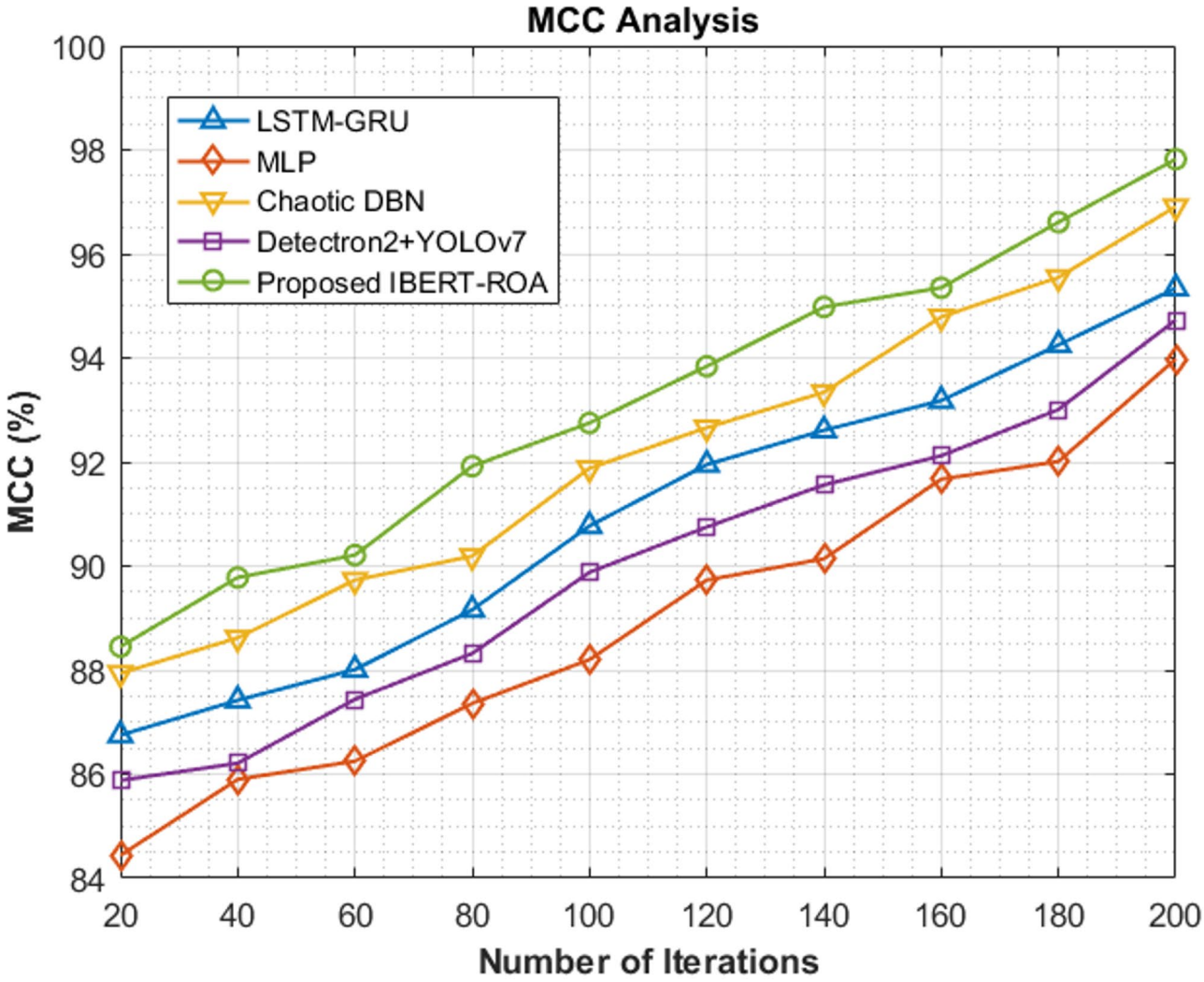

Fig. 9. MCC analysis.

Confusion matrix

The confusion matrix presented in Fig. 12 offers a detailed evaluation of the classification outcomes achieved by the proposed IBERT-ROA model on the test dataset. The matrix captures true positives along the diagonal and illustrates how well each of the nine classes, namely, Benign, HTTP Flood, ICMP Flood, SYN Flood, SYN Scan, Slowrate DoS, TCP Connect Scan, UDP Flood, and UDP Scan—were identified by the classifier. Notably, the majority of instances across all classes were correctly classified, demonstrating the model's strong discriminative power. For example, 95,170 out of 95,189 benign samples were accurately identified, while malicious classes such as HTTP Flood and UDP Flood achieved perfect or near-perfect prediction scores with minimal misclassification. Misclassifications were primarily observed in closely related categories, such as SYN Scan versus TCP Connect Scan, where structural similarity in traffic patterns may cause minor ambiguity. Nonetheless, the overall high diagonal dominance of the matrix confirms that the IBERT-ROA model effectively generalizes across diverse attack types and benign traffic, maintaining both high sensitivity and specificity.

The TP, TN, FP, and FN breakdown provided in Table 3 offers a granular assessment of the classification behavior of the IBERT-ROA model. It reveals how accurately the model identifies each class and highlights areas where minor misclassifications occur.

For example, the Benign class has 95,170 true positives and only 19 false negatives, indicating strong detection ability with minimal misclassification. Similarly, HTTP Flood shows perfect classification with no false positives and only 4 false negatives, reflecting the model's robustness in identifying high-volume flood-based threats. In classes like SYN Scan and TCP Scan, a small number of false positives and false negatives are observed, which may arise from behavioral similarity in traffic patterns. Notably, the ICMP Flood class records a perfect recall (0 FN) and nearly zero false positives, highlighting the model's precision in detecting even under-represented attack types. These values validate the superior performance of IBERT-ROA, especially in minimizing false positives (critical in network trust maintenance) and false negatives (essential for robust security). Overall, the TP/TN/FP/FN metrics affirm that the model generalizes well and is suitable for real-time deployment in cognitive 5G networks.

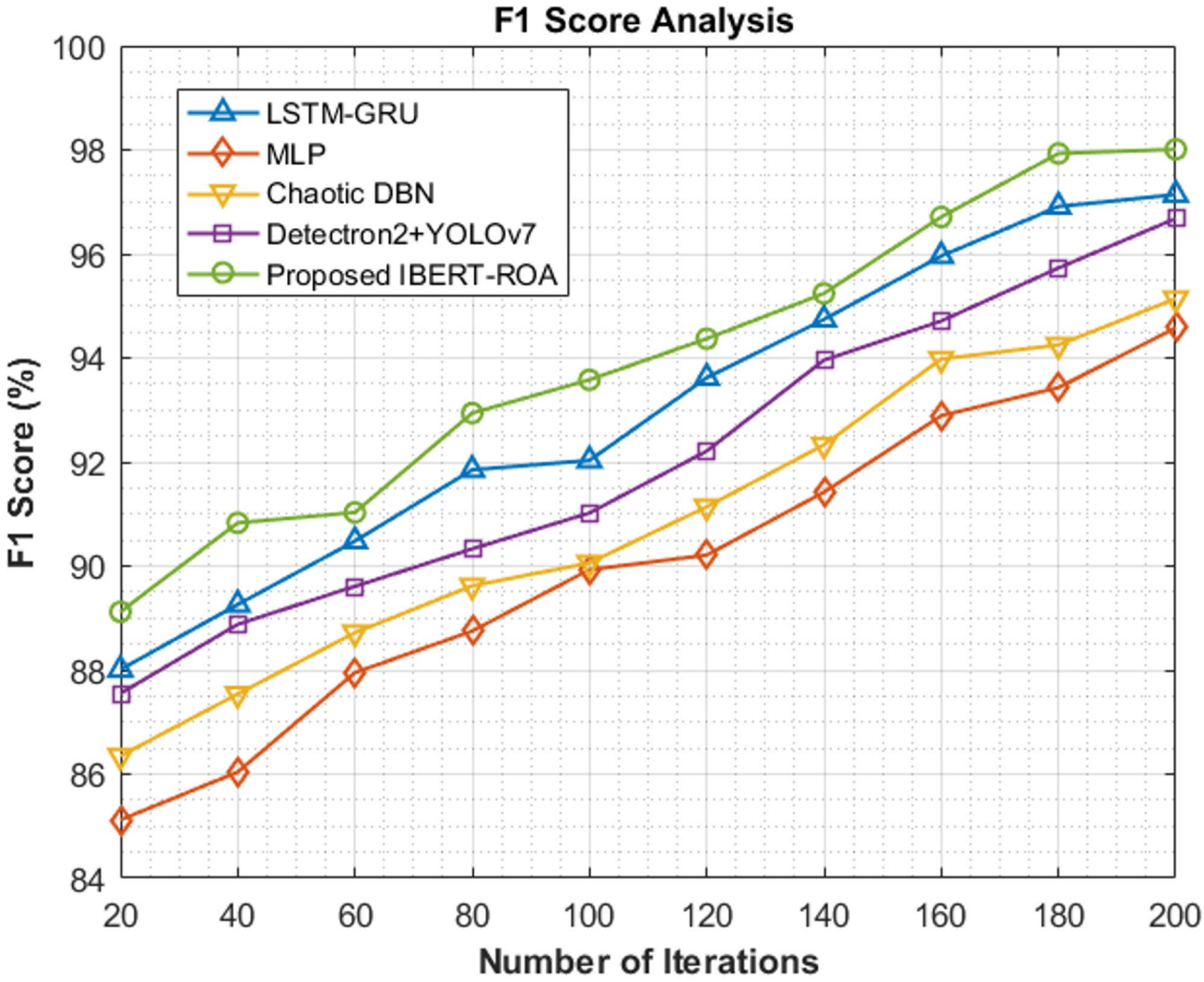

Fig. 10. F1 Score analysis.

Table 4 provides a comparative view of the precision and recall metrics computed separately for the training and testing phases of the proposed IBERT-ROA model. The values reflect class-wise performance consistency and model generalization from training to deployment.

Table 4 presents a detailed comparison of precision and recall for both training and testing phases across all nine classes. The minimal variation observed between training and testing metrics indicates strong generalization of the IBERT-ROA model and confirms that overfitting is not present. For instance, the Benign class achieves a training precision of 99.40% and testing precision of 98.91%, with recall values of 99.20% and 98.48%, respectively. Classes with rare occurrences, such as ICMP Flood, still achieve near-perfect recall in testing (100.0%) and maintain precision above 98.5%, showcasing the model's effectiveness in handling imbalanced datasets. The SYN Scan and TCP Scan classes show slightly lower test-phase precision (98.15% and 98.45%) but compensate with high recall (99.88% and 99.85%), which is crucial in minimizing false negatives. These results underscore the IBERT-ROA model's capability to retain classification fidelity even when deployed outside the training domain, confirming its robustness for real-time malicious user detection in cognitive 5G environments.

comparison analysis

The comparison with the existing methods to confirm the value and contribution of the proposed work is described below in Table 5.

discussion

The comparison linked to the effectiveness of the MUC-C5GN model perfectly indicates that the offered IBERT-ROA explains a better option of MUC-C5GN. The model outperforms the classical methods steadily: LSTM-GRU, MLP, Chaotic DBN and Detectron2 + YOLOv7 in all crucial metrics: the accuracy, sensitivity, FPR, precision, MCC, F1 Score and specificity. IBERT-ROA is performing quite well on learning, generalization and convergence abilities, as IBERT-ROA reaches the highest final scores on all of the criteria after 200 iterations as well. What makes it even more reliable in high-stakes and real-time conditions is its remarkable accuracy along

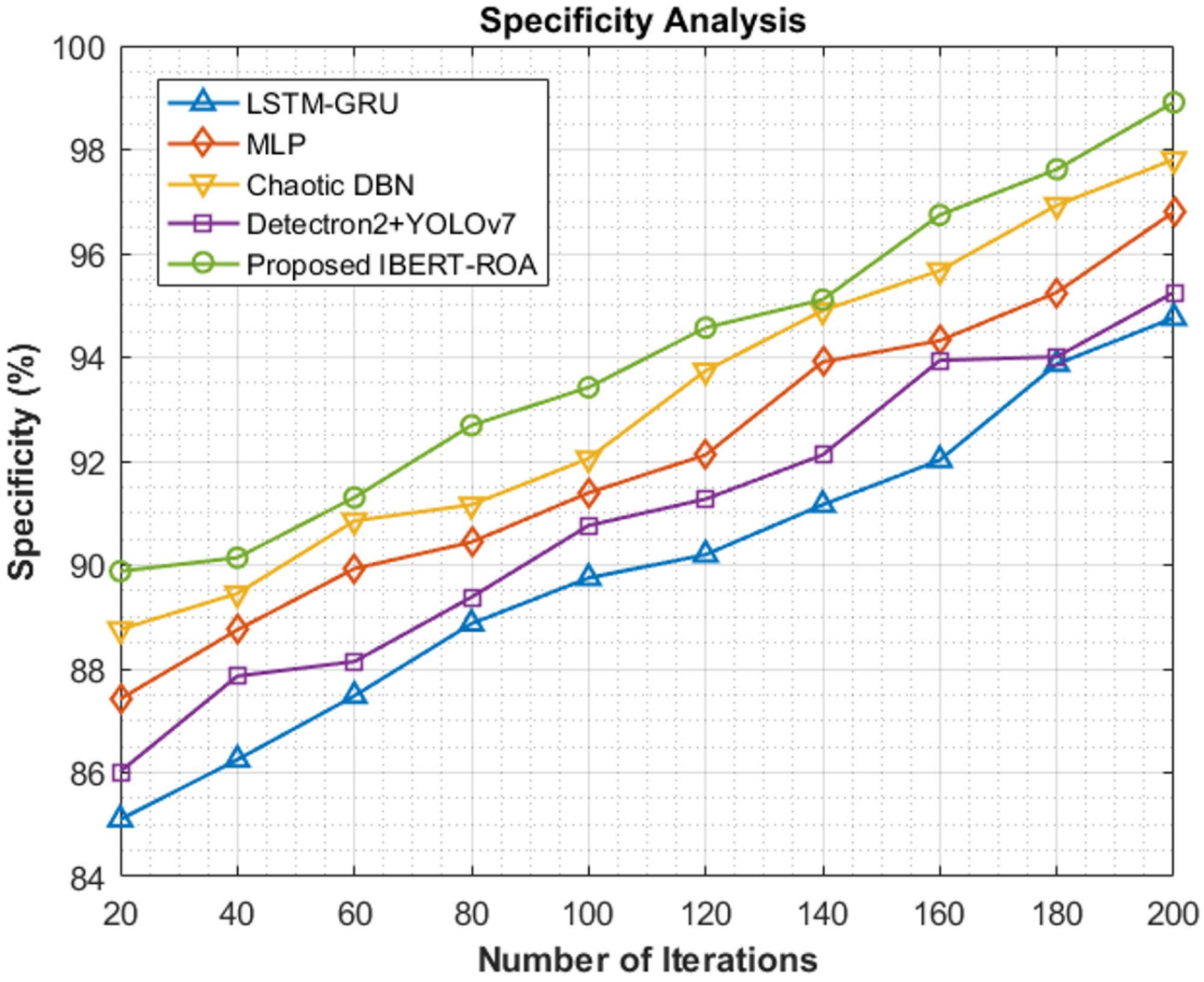

Fig. 11. Specificity analysis.

with the F1 Score, and how the case with the FPR being quite low and specificity being quite high validates its effectiveness in the realm of categorizing malicious and legitimate users. Its competitive nature is also solidified by the estimated percentages of advantages as compared to other models. These findings point to a relevant potential of IBERT-ROA applications in dynamic, safe 5G cognitive systems, where the confidence of users and network integrity are supported by fast, precise, and scalable threats identification.

Conclusion

The MUC-C5GN was carried out in this work using a novel intelligent optimization technique that was centered on machine learning. Initially, the data was collected via the 5G-NIDD standard benchmark resources. The gathered data was processed using scaling as well as normalization algorithms. This pre-processed data was then subjected to feature extraction using the Self-Attention RNN-AE approach. Finally, malicious users in cognitive 5G networks were classified using the new IBERT model. ROA, a nature-inspired optimization technique, was used to change the settings of BERT. For the whole MUC-C5GN model, maximizing accuracy was considered the fitness function. According to simulation data, the suggested MUC-C5GN model fared better than the other existing approaches that were looked at across a number of measures. For the MUC-C5GN model, the proposed IBERT-ROA outperformed existing techniques by 5.99% in sensitivity as well as 2.74% in accuracy.

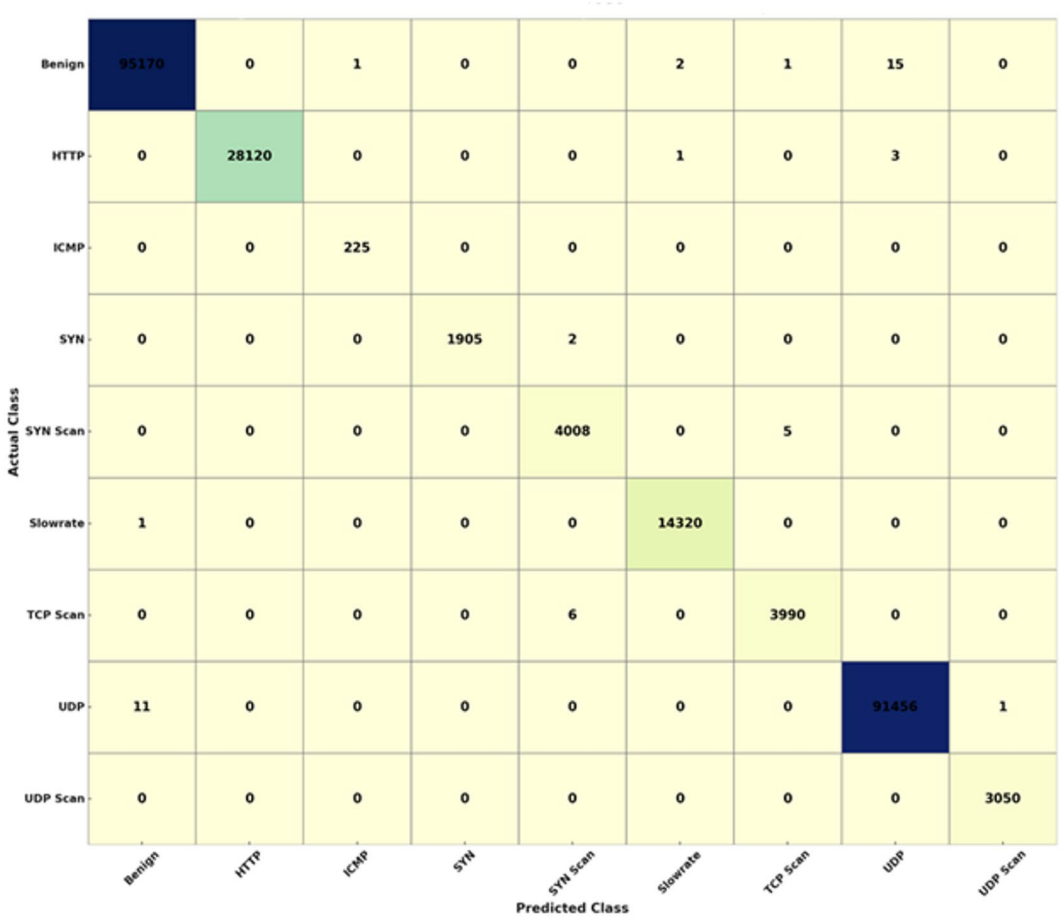

Fig. 12. Confusion matrix analysis.

Class	True Positives (TP)	True Negatives (TN)	False Positives (FP)	False Negatives (FN)	Class
Benign	95,170	147,092	12	19	Benign
HTTP	28,120	214,169	0	4	HTTP
ICMP	225	242,067	1	0	ICMP
SYN	1905	240,386	0	2	SYN
SYN Scan	4008	238,272	8	5	SYN Scan
Slowrate	14,320	227,969	3	1	Slowrate
TCP Scan	3990	238,291	6	6	TCP Scan
UDP	91,456	150,807	18	12	UDP
UDP Scan	3050	239,242	1	0	UDP Scan

Table 3. TP, TN, FP, and FN values for each class in the test Phase.

Class	Precision (Train)	Precision (Test)	Recall (Train)	Recall (Test)
Benign	99.4	98.91	99.2	98.48
HTTP	99.55	99.45	99.6	99.3
ICMP	98.95	98.66	98.9	100
SYN	99.1	98.7	98.95	98.96
SYN Scan	98.82	98.15	98.95	99.88
Slowrate	99.35	99.1	99.42	99.42
TCP Scan	98.8	98.45	98.6	99.85
UDP	99.6	99.35	99.55	99.64
UDP Scan	98.75	98.5	98.6	99.87

Table 4. Training vs. Testing precision and Recall.

Citation	Dataset	Methodology	Performance metrics	Features and shortcomings
[28]	5G-NIDD (5G testbed flows)	Transformer IDS (self-attention for multi-class intrusion; non-IP data delivery)	Accuracy 99.49%; CNN-based baseline lower; RNN baseline 99.91% but slower	Confirms Transformer dominance on 5G-NIDD; small gaps vs. RNN but better runtime/robustness.
[29]	Custom 5G testbed	Pretrained Transformers (DistilBERT, RoBERTa, ALBERT) + contrastive learning; projection head	High accuracy/precision/recall/F1 score(DistilBERT/RoBERTa/ALBERT > BERT)	Strong unsupervised separation; depends on attack diversity in testbed; calculate cost for large encoders.
[34]	N-BaIoT (IoT access side)	Edge-deployed Transformers at multiple detection points + personalized federated learning (parameter sharing)	Accuracy 99.2%, F1 score 99.2% (avg across sites)	Comparable to centralized training; added coordination/communication overhead across nodes.
[35]	VeReMi-extension (V2X)	Transformer at 5G edge, federated learning, personalization for site-specific behavior	Accuracy 99.37%, Recall 98.69%, F1 score 99.30%	Robust to attacks mimicking legitimate behavior; edge compute + FL synchronization needed.
[37]	5G-V2X	Self-Supervised Pretraining on unlabeled data + minimal labeled fine-tuning	Up to + 9% accuracy gain vs. supervised baselines (varied sizes; as low as 200 samples)	Strong when labels are scarce; depends on unlabeled data diversity and expert-crafted small label set.
Proposed IBERT-ROA	5G-NIDD	Self-Attention RNN-AE - IBERT-R classifier, optimized via ROA (temporal feature distillation - contextual transformer encoding -hyperparameter/feature/attention search)	Accuracy: 99.74, sensitivity: 98.48, FPR: 1.16, precision: 98.91, MCC: 97.82, F1 Score: 98.01, specificity: 98.91	Integrates sequential anomaly cues (RNN-AE), contextual semantics (IBERT-R), and automated tuning (ROA) for real-time 5G. (Dataset details: 1,215,890 flows; 9 classes; 112 features.)

Table 5. Comparison of the proposed model with existing models.

Data availability

The datasets generated and/or analyzed during the current study are available in the 5G-NIDD repository, [https://ieee-dataport.org/documents/5 g-nidd-comprehensive-network-intrusion-detection-dataset-generated-over-5 g-wireless#files].

Received: 19 July 2025; Accepted: 5 September 2025
Published online: 09 December 2025

References

1. Lilhore, U. K., Dalal, S. & Simaiya, S. A cognitive security framework for detecting intrusions in IoT and 5G utilizing deep learning. *Computers Secur.* **136**, 103560 (2024).
2. Ahmed, A. et al. A comparative analysis of different outlier detection techniques in cognitive radio networks with malicious users, Wirel. Commun. Mob. Comput, vol. 2020. (2020).
3. Almuqren, L. et al. Optimal deep learning empowered malicious user detection for spectrum sensing in cognitive radio networks. *IEEE Access.* **12**, 35300–35308 (2024).
4. Taggu, A. & Marchang, N. Detecting Byzantine attacks in cognitive radio networks: A two-layered approach using hidden Markov model and machine learning. *Pervasive Mob. Comput.* **77**, 101461 (2021).
5. Wu, W. et al. Joint sensing and transmission optimization for IRS-assisted cognitive radio networks. *IEEE Trans. Wireless Commun.* 5941–5956 (2023).
6. Salahdine, F. & Kaabouch, N. Security threats, detection, and counter measures for physical layer in cognitive radio networks: A survey. *Phys. Commun.* **39**, 101001 (2020).
7. Sureka, N. & Gunaseelan, K. Investigations on detection and prevention of primary user emulation attack in cognitive radio networks using extreme machine learning algorithm. *J. Ambient Intell. Humaniz. Comput.* 1–24 (2021).
8. Elghamrawy, S. M. Security in cognitive radio network: defense against primary user emulation attacks using genetic artificial bee colony (GABC) algorithm. *Future Gener Comput. Syst.* **109**, 479–487 (2020).
9. Kumar, G. P. & Reddy, D. K. Hierarchical Cat and mouse based ensemble extreme learning machine for spectrum sensing data falsification attack detection in cognitive radio network. *Microprocess Microsy.* **90**, 104523 (2022).
10. Turkyilmaz, Y., Senturk, A. & Bayrakdar, M. E. Employing machine learning based malicious signal detection for cognitive radio networks. *Concurr Comput. Pract. Exp.* **35**, 7457–7471 (2022).
11. Zhang, Y., Wu, Q. & Shikh-Bahaei, M. R. On ensemble learning-based secure fusion strategy for robust cooperative sensing in full-duplex cognitive radio networks. *IEEE Trans. Commun.* **68**, 6086–6100 (2020).

12. Soundararaj, A. J. Godfrey winster sathianesan,task offloading scheme in mobile augmented reality using hybrid Monte Carlo tree search (HMCTS). *Alexandria Eng. J.* **108**, 611–625 (2024).
13. Samson, S., Arivumani & Nagarajan, M. Adaptive convolutional-LSTM neural network with NADAM optimization for intrusion detection in underwater IoT wireless sensor networks, Engineering Research Express, vol. 6, Septembr (2024).
14. Janani, S., Ramaswamy, M. & Samuel Manoharan, J. An optimized congestion retrieval mechanism for cognitive radio sensor network. *J. Comput. Theor. Nanosci.* **16** (4), 1563–1572 (2019).
15. Janani, S., Ramaswamy, M., Samuel Manoharan, J. & Clustered HEED scheme for congestion avoidance in cognitive radio sensor network. *J. Theoretical Appl. Inform. Technol.* **96** (17), 5674–5684 (2018).
16. Manish Kumar, G. & Saikat majumder, extreme learning machine based identification of malicious users for secure cooperative spectrum sensing in cognitive radio networks. *Wireless Pers. Commun.* **130**, 1993–2012 (2023).
17. Minilal, M. & Meena, M. January, Security threat analysis in 5G cognitive radio networks: A deep learning ensemble approach. *Int. Inform. Eng. Technol. Association* **15**, 181–187 (2025).
18. Gang, H. H., Ma, Z. Z. Z. Y. & Yang, T. AI-Based Malicious Encrypted Traffic Detection in 5G Data Collection and Secure Sharing, Electronics, vol. 14, no. 1, (2025).
19. Kouchaki, M., Zhang, M., Abdalla, A. S., Lan, G. & Brinton, C. G. Vuk Marojevic,Enhanced Real-Time Threat Detection in 5G Networks: A Self-Attention RNN Autoencoder Approach for Spectral Intrusion Analysis, Cryptography and Security, November (2024).
20. Zihao Wang, K. W. & Fok, V. L. L. *Thing,Exploring Emerging Trends in 5G Malicious Traffic Analysis and Incremental Learning Intrusion Detection Strategies* (Cryptography and Security, February 2024).
21. Marriwala, N. K. et al. OntoBlock: a novel ontological-based and blockchain enabled spectrum sensing framework for detection of malicious users in cognitive radio internet of things (CR-IoT) networks. *Int. J. Inform. Technol.* **16**, 3913–3921 (June 2024).
22. Minilal, M. & Meena, M. AI driven security threat analysis for 5G cognitive radio short range applications. *Int. J. Intell. Syst. Appl. Eng.* **12**, 68–73 (2024).
23. Du, H. & Chen, L. Jegatha Deborah,A Collaborative Spectrum Sensing Algorithm Based on Reputation Update against Malicious User Attacks, Security and Communication Networks, vol. 2023. (2023).
24. Malgorzata Wasilewska, H. & Bogucka, H. Vincent poor, secure federated learning for cognitive radio sensing. *Signal Process.* **61** (3), 68–73 (2023).
25. Sefa Kayraklik, I., Yildirim, E., Basar, I. & Hokelek. Ali gorcin, practical implementation of RIS-aided spectrum sensing: A deep learning-based solution. *Signal Process.* **18** (2), 1481–1488 (2024).
26. Evelyn Ezhilarasi, J. & Christopher Clement, G. R. U. S. V. M. Based Threat Detection in Cognitive Radio Network, Sensors, vol. 23, no. 3, January (2024).
27. Kumar, A., Vrizlynn, L. L. & Thing *Malicious Lateral Movement in 5G Core with Network Slicing* (110–117) (And Its Detection, Cryptography and Security, December 2023).
28. Kumar Harshdeep, K., Sumalatha, R. & Mathur June, DeepTransIDS: Transformer-Based deep learning model for detecting DDoS attacks on 5G NIDD. *Results Eng.* **26**, 104826 (2025).
29. Sheikhi, S., Kostakos, P. & Pirttikangas, S. Effective Anomaly Detection in 5G Networks via Transformer-Based Models and Contrastive Learning, 2024 8th Cyber Security in Networking Conference (CSNet), Paris, France, pp. 38–43, 2024. (2024).
30. Alsharaiah, M. A. et al. An explainable AI-driven transformer model for spoofing attack detection in internet of medical things (IoMT) networks. *Discov.Appl. Sci.* **7**, 488 (2025).
31. Shahriar, A. et al. 5GPT: 5G vulnerability detection by combining Zero-Shot capabilities of GPT-4 with domain aware strategies through prompt engineering. *IEEE Trans. Inf. Forensics Secur.* **20**, 7045–7060 (2025).
32. Ankur, G. & Dinesh Chandra Misra, Hybrid IoT security model with integration of LSTM, BERT, ROBERTA and transform learning for attack classification, International Journal of Information Technology, August (2025).
33. Saeed Alketbi, K. & Mehmood, A. A Comprehensive Survey of Explainable Artificial Intelligence Techniques for Malicious Insider Threat Detection, IEEE Access, vol. 13, pp. 121772–121798, (2025).
34. Luo, Y. et al. Securing 5G/6G IoT using transformer and personalized federated learning: an Access-Side distributed malicious traffic detection framework. *IEEE Open. J. Commun. Soc.* **5**, 1325–1339 (2024).
35. Missara, R. et al. Misbehavior Detection System in V2X 5G Edge Networks based on Transformer, 2025 Global Information Infrastructure and (GIIS), Dubai, United Arab Emirates, pp. 1–6, 2025. (2025).
36. Fuzel Jamil, A. et al. Secure provenance using an authenticated data structure approach, *Computers Secur.*, **73**, 34–56, March (2018).
37. Hossain, S. & Senouci, S. M. January, Bouziane brik, and Abdelwahab boualouache,a privacy-preserving Self-Supervised Learning-based intrusion detection system for 5G-V2X networks. *Ad Hoc Netw.*, **166**, 103674 (2025).

Author contributions

Saranya S – Research proposal – construction of the work flow and model – Final Drafting; N.Malligeswari – Survey of Existing works – Improvisation of the proposed model; F.Twinkle Graf – Initial Drafting of the paper – Collection of datasets and choice of their suitability – Formulation of pseudocode; V.Murugan– Survey of Existing works –Supervising of full manuscript and Finding the Novelty methodology.

Funding

The author did not receive support from any organization for the submitted work.

Declarations

Competing interests

The authors declare no competing interests.

Conflict of interest

The author has no relevant financial or non-financial interests to disclose.

Additional information

Correspondence and requests for materials should be addressed to S.S.

Reprints and permissions information is available at www.nature.com/reprints.