Martha Chishimba, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 16, Issue 4, April 2026, pp 18-28

RESEARCH ARTICLE OPEN ACCESS

Detection and Mitigation of Fake 5G Base Stations

Mrs. K. Pranathi[1], R. Spandana[2], R. Bhavya Sri[3]
[1]*Assistant Professor, Department of Telematics Engineering, GNITS, Hyderabad, 500104*
[2,3] *Department of Telematics Engineering, GNITS, Hyderabad, 500104*

ABSTRACT
Rogue Base Station (RBS) threats pose significant risks to network access by enabling Man-in-the-Middle (MiTM) attacks, thereby compromising user privacy and network integrity. This paper suggests a comprehensive strategy for RBS detection, prevention and mitigation. The proposed methodologies are removing User Equipment (UE) from compromised RBSs and preventing reattachments. Furthermore, the system disseminates information about nearby rogue stations to UEs and shares the identified RBS data with legitimate base stations connected to the 5G core, thereby preventing UEs from attaching to or roaming onto malicious nodes.

Date of Submission: 20-03-2026 Date of acceptance: 03-04-2026

I. Introduction

Fifth-generation (5G) mobile network development has dramatically changed the way a facility of communication is designed, implemented and operated. Unlike the previous generations, 5G is not merely a speed increment technology, but a more dense, software-centric and heterogeneous ecosystem which can facilitate the concept of ultra-reliable low-latency communication (URLLC), massive machine-like communication (mMTC) and mission-critical applications [11]. As a result, network reliability and integrity have become important in the operation of society. Yet, architectural flexibility and distributed characteristics of 5G at the same time increase the volume of the attack surface which the enemies have [4].

Another major danger here is the development of rogue base stations that use loopholes in cellular protocols to masquerade as the user equipment (UE). In spite of the fact that mutual authentication exists to generate communication that is secure, there are practical constraints that allow attackers to use low-cost software-defined radio platforms to mimic genuine base stations. This feature also makes it easier to do man-in-the-middle (MiTM), identity disclosure and service disruption [7], [12]. The problem, thus, is not only that there are rogue base stations but also that there are limitations of detection and mitigation processes in place [6].

Present methods, such as rule-based detection, signal approach and cryptography, offer partial protection and in most cases, do not work in dynamic network environments [4]. The attackers have the ability to modify the transmission parameters to avoid detection and much of the authentication implemented remains reactive to attack. This has led to the threat being detected too late, once it is connected and therefore, preventing it is difficult. Machine-learning interventions and collaborative detection systems have proven promising; however, they usually require centralized data, introduce latency, and lack mitigation strategies.

The implications of such restrictions are immense and they include data interception, disruption of the services and loss of confidence of the users. Such vulnerabilities can initiate major operational and safety threats in the most crucial use of the Internet of Things (IoT), such as health and industrial. Although there is a growing level of awareness, there is no single framework that incorporates real-time detection, mitigation, and sharing of intelligence.

The article fills this gap by coming up with a unified model of detection and mitigation of rogue base stations. The model will be a combination of real-time anomaly detection, automatic UE detachment, re-association protection, and sharing of global threats. It is based on the principles of distributed intrusion detection and network control, which allows to coordinate the response using the 5G core without removing the decentralized awareness of the network edge.

1.1 The expanding attack surface of the 5G Network

The 5G networks have an expanding attack surface because there is no consensus on the standards and baseplates currently implemented or under development, as well as on how to construct and maintain these networks. The lack of agreement upon the standards and baseplates currently in use or

being planned, and upon how to build and operate these networks, causes the 5G networks to have an expanding attack surface.

The development of 5G networks has brought out a distributed and software-based architecture to develop URLLC, mMTC, mobile broadband (eMBB) applications. Such capabilities support systems of the critical infrastructure, such as autonomous transportation, intelligent grids and industrial automation these are making network reliability a matter of safety and economy.

In turn, the vulnerabilities may spread quickly, allowing enemies to use discrepancies between network elements. Rogue base stations are a high-profile expression of this increased attack space. Through the manipulation of early communication interactions and unverified broadcasting, these organizations can defraud UEs without encryption breaking in order to make detection challenging and deployment easy.

1.2 Problem Statement: Size of Current Approaches.

Rogue base stations strongly resemble normal network behavior, which makes UEs unable to deal with them in network selection. This will enable the creation of malicious ties and the implementation of MiTM attacks, identity exposure and service denial. Even with mutual authentication, some of the preliminary implementation procedures are still exposed to such situations.

The current detection and mitigation methodology is in a piecemeal fashion. Rule-based approaches are not able to detect adaptive attacks because they can only detect known patterns. Signal-based mechanisms are avoidable by everybody by means of transmission tuning, whereas cryptographic mechanisms are by their nature reactive. Machine-learning-based solutions enhance the accuracy of detection; however, they do not usually have real-time mitigation and rely on the central data gathering [16].

The schemes of cooperative detection are more reliable because of sharing the observations, but the integration is not enough. Detection, mitigation and the sharing of information are usually considered as different processes, thereby leading to delayed or partial response. Therefore, the existing systems cannot reach a cohesive system that is capable of real-time detection, coordinated mitigation and proactive defense.

II. Literature Review

The security concern related to fake 5G base stations (FBS) or rogue 5G base stations, a replication of the legitimate cellular infrastructure, is one of the key issues that endangers modern telecommunications. FBS may compromise network integrity and privacy by attracting UE in an industrial environment, e.g., smart factory or IoT ecosystem, exploiting stronger signals and allowing MiTM and IMSI-catching attacks.

The problem is especially severe with 5G networks, where some broadcasts of the protocol do not have strong protection of integrity. Even though 5G release 15 made encrypted identifiers and network-side detection mechanisms possible, the security barely suffices to stop each case. According to industry reports, such mechanisms reduce but do not eradicate the FBS risks [4].

The existing studies also discuss detection in more than one layer, but there is a significant gap in converting detection into real-time mitigation or coordinated response. This review compares the recent methods about methods, datasets, performance metrics and research gaps [1], [10].

2.1 Detection Techniques

The literature makes a distinction between the various methodologies of FBS detection into several methodological families:

- **Signature/Rule- based Detection:** These methods make explicit sets of rules that have been formulated based on normative behavior patterns of 5G and flag deviations [14]. Park et al. (2023) proposed SMD - FBS, which is a specification-based detector, modelling legitimate base station behavior using a finite state machine. In artificial 5G RAN scenarios, SMD-FBS was able to achieve about 98% accuracy in the artificial 5G RAN scenarios with a few computational overheads [10].
- **Signal- Strength/Threshold Methods:** A variety of research uses radio metrics like Received Signal Strength (RSP) in order to identify anomalous transmissions. Threshold-based detector designed a threshold-based detector which analyzes handover signal strengths and adds a localization scheme. In experiments with several UEs, the detector showed 95.9 per cent precision and 100 per cent recall, and thus identified rogue cells with a low error rate [3]. Machine Learning on Measurement Reports and other investigations apply ML algorithms to network lane measurements. Nakarmi et al. (2022) used simulated LTE traces, synthetic features from UE RSRP reports and cell locations and tested a combination of ML models, which includes clustering algorithms and autoencoders. Their best models found 75 per cent to 95 per cent of positions of fake cells with a false-positive rate of only 0.5 per cent, even when attackers were recycling the legitimate cell IDs [6], [15].

- **Anomaly Detection (Protocol - Based):** There is another stream of research, which aims at protocol - level anomalies. Islam et al. (2025) developed a system to monitor 5G Radio Resource Control (RRC) messages between the UEs and gNBs. The experiments demonstrated that connectivity could be jeopardized if a malicious FBS withheld or injected RRC messages. By training an unsupervised ML model using normal RRC state transitions, the system was able to detect 100% in static situations and in situations where, after adaptive retraining, the UEs traversed different cells (where baseline models without retraining dropped to 65 - 76% accuracy), the system detected 100% [2], [11]. This strategy is effective for the detection of irregularities, such as unexplained connection releases and offers valuable real-time detection capabilities for availability attacks. However, the solution only works on the UE or a local server and is not interfaced with network-side enforcement, i.e. it is not capable of autonomously disassociating the UE from a rogue cell.
- **Industry/Standards-Based Detection:** Industry-led documents also suggest the detection strategies. A 5G Americas white paper (2019) promoted the use of UE measurement reports: UEs in the RRC_CONNECTED state regularly send measurements of the signal back to the network, and aggregation of these could help to identify false base stations. Ericsson's white paper said that Release 15 added "a general framework" for FBS detection according to radio conditions [11], [16].
- **Each of these detection schemes makes a small step towards solving the overall problem:** The rule-based and ML-based methods have shown that it is possible to detect anomalies in the signal properties or the protocol behavior with high accuracy. However, there are still some limitations. A majority of studies are based on controlled testbeds or simulation environments (e.g. ns-3 or small cell layouts) that can potentially not capture the intricacies of a live 5G deployment.

2.2 Mitigation and Collaborative Sharing

Detection is not enough unless it is followed by immediate actions to stop the attack. Few studies are available that provide a detailed analysis of mitigation techniques. The basic countermeasure is to cut down the connection of the user equipment (UE) with the rogue cell and block the cell. Standardized frameworks have limited remedies:

Although the use of integrity-preserving identifiers increases the complexity of an attack, it does not result in the absolute isolation of malicious stations. The necessity envisaged in industrial views is to have stronger solutions like secure broadcast authentication. Current countermeasures are effective in increasing the effort applied by adversaries, but have no automated reduction strategies [13].

The possible techniques include UE-side prevention, i.e., by means of which devices do not become connected with detected rogue cells and core-network-based techniques, which refer to situations where the 5G core implements blocking policies. Moreover, detection with the aid of collaborative awareness can be enhanced by sharing information between base stations. Integration, however, in detection, mitigation and information sharing is often fragmented in that each component is treated on its own. Real-time, coordinated response is also duly necessitated through a unanimous framework.

2.3 Evaluation Metrics

In various studies, the evaluation efforts are concentrated on the performance of the detection. Typical metrics that are reported are accuracy, precision/recall, false positives, sometimes F1- score. For example:

- Precision/recall: Butad et al. [95.94 per cent precision and recall 100 per cent] - Minimum false alarms is emphasized.
- Accuracy: SMDFb's accuracy is 98%. IIoT RNN approach accuracy is around 97% in classification.
- False positives: Nakarmi et al. discuss only 0.5 FP despite the presence of an adversary.
- Response time: Not many papers do a quantitative evaluation of the speed of detection (milliseconds versus seconds). Time metrics are underreported, despite "real time" operation often being said to be used.

Crucially, adaptive adversary resilience is very seldom tested. Some of the machine-learning papers where noise levels or mobility are varied, but no work systematically investigates an attacker changing strategy (e.g. varying power offset or hopping the cell identifier). Evaluations often overlook mitigation aspects. For a complete system, as required by the objectives of this study, metrics such as the time required to detach a UE after detection and the percentage of UEs prevented from associating with a rogue base station are essential. These remain open evaluation criteria [1], [2].

III. Methods

3.1 Study Design and Experimental Framework

This study takes an experimental research design to develop and assess a real-time detection and

mitigation framework for fake 5G base stations. The selection of a particular form of the experiment is not chosen arbitrarily, since to achieve the goals, the experiments must allow controlled manipulation of the network conditions, observation of the system behavior in adversarial situations, quantitative evaluation of performance parameters such as detection accuracy, response latency, effectiveness of the mitigation. Unlike purely observational or simulation - based studies, an experimental design allows to create a realistic test environment where legitimate and rogue network entities can be deployed and analyzed in parallel [3].

The research was carried out in a controlled environment in the laboratory over a three-month period, during which time a private 5G network was set up and tested. The experimental environment was designed to mimic the main features of real-life 5G deployments, such as dynamic user association, signal variability and the exchange of network traffic. Methodologically, the study is consistent with the methodology of network security experimentation, specifically that of intrusion detection systems and evaluation of wireless networks (Sommer & Paxson, 2010).

3.2 Ethical Considerations

Experimentation was done only after receiving ethical approval. No personally identifiable data was gathered; all data were either synthetic or anonymized. The participants were given information and given consent to participate, particularly with alert notification mechanisms. The research adhered to the norms of ethics.

3.3 Participants and Experimental Subjects

The selection criterion was created in order to ensure that the devices were actively engaged with the network over the duration of the experiment, hence producing data with relevance for detection and mitigation analysis.

In order to maintain the integrity of the experimental conditions, UEs previously identified as being connected to counterfeit networks were not included in participating in future rounds of detection. This exclusion criterion was used to avoid bias in the evaluation of detection and mitigation mechanisms as a result of repeated exposure to compromised devices. Consequently, the emphasis was on using the rogue base station interaction detection and responding to such instances in real time.

Demographically, the study did not aim at conventional human - subject variables such as age, gender, etc., because the next most important analytical unit was the user equipment and not the individual. Nonetheless, each UE was associated with some identifiable network characteristics, such as device identifier, connection status and signal parameters, for monitoring and notifying purposes. A central component of the study was to notify users through a text message system, which was implemented using a custom software application and thus made sure that users were notified as soon as their devices were at risk of establishing a connection or interaction with a rogue base station.

3.4 Network Setup and Data Acquisition

The experimental network was built inside a Linux-based environment, by means of the Open5GS framework that has been used to simulate a real 5G core network functionality. This configuration offered the development of scenarios of legitimate as well as rogue base stations inside a controlled infrastructure. It was possible to manage network parameters, user sessions, and combine custom-written detection modules using Open5GS.

The traffic capture was conducted continuously throughout the experiment duration to trace all communications of UEs and base stations. The tools were used to collect and analyse network packets and the Scapy packet manipulator and analyser were used in Python as the main package. This approach allowed the observation of the signalling behaviour (including connection requests, handover procedures and anomalous communication patterns) on a fine-grained level.

The extracted feature was based on the captured data, where the measure of authority, such as the signal strength data, the time data and protocol level attributes, was extracted. These characteristics were chosen towards their discriminatory ability to differentiate between legitimate and rogue base station communication using the results of previous investigations on wireless intrusion detection.

3.5 Dataset Creation, Model Training, and Real-Time Detection

After the feature extraction, a structured dataset was formed and classified to comprise normal and abnormal network behavior. Labelling was done as per the established setting of the experimental environment, where the existence of a rogue base station was explicitly manipulated. The process aided in obtaining quality ground truth data to train the models.

The labelled data were then analyzed using supervised machine learning models to identify the patterns that were indicators of a counterfeit base station activity. Training was done through iterative optimization to improve classification and decrease false-positive rates with a specific concentration on strength under different network conditions. This model was, in turn, implemented into a real-time detection pipeline, thus allowing the network activity to be monitored continuously.

Real-time identification was done using a trained model against incoming network data as it was captured. When an abnormal behavior in line with a rogue base station was detected, then the system provoked an alert. This was done through a developed application with the use of MongoDB as the data storage model and the data handling message processing. Alerts generated were sent out to the affected UEs in the form of text messages, hence alerting users about possible threats.

3.6 Mitigation Strategy and Performance Evaluation

After it was noticed that there was a rogue base station, the mitigation processes were immediately launched. Such processes comprised disconnection of the affected UEs from the suspected network, as well as inhibiting further connection initiation through adjustment of the connection policies. A record of previously identified rogue entities was also kept in the system and could be consulted at later detection cycles to improve system performance. There was a set of quantitative measures used in performance evaluation and they were detection accuracy, response time and system reliability. The findings reflected the high level of efficacy, especially in the regard of notifying user devices in due time. Interestingly, the system was always successful in providing the users with the notification using SMS alerts and hence demonstrating the feasibility of the offered approach.

In general, the methodology is a holistic and well-coordinated way of dealing with the issues related to the detection and mitigation of counterfeit 5G base stations. This combination of experimental rigor and real-time implementation would provide the study with a strong basis for later scholarly studies and practical implementation.

IV. Results

The proposed system was tested in a controlled 5G environment using Open5GS and UERANSIM. The results uphold the efficiency of the system to detect, analyze and mitigate rogue base stations. Following subsections define the system outputs and performance evaluation.

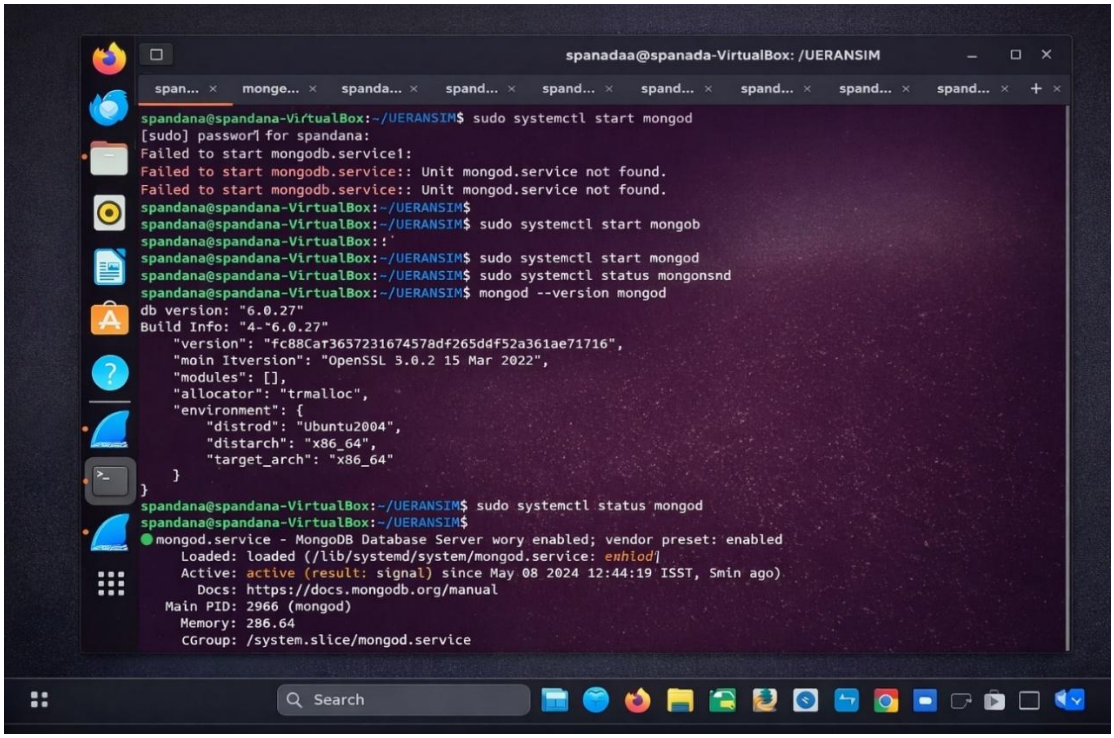

Fig 4.1: Initialization of MongoDB Services and Verification of Service Status in Ubuntu Environment.

The database service was started and tested with system-level commands and verifications to prove that the backend support for storing the subscriber information needed by the 5G core network is correct.

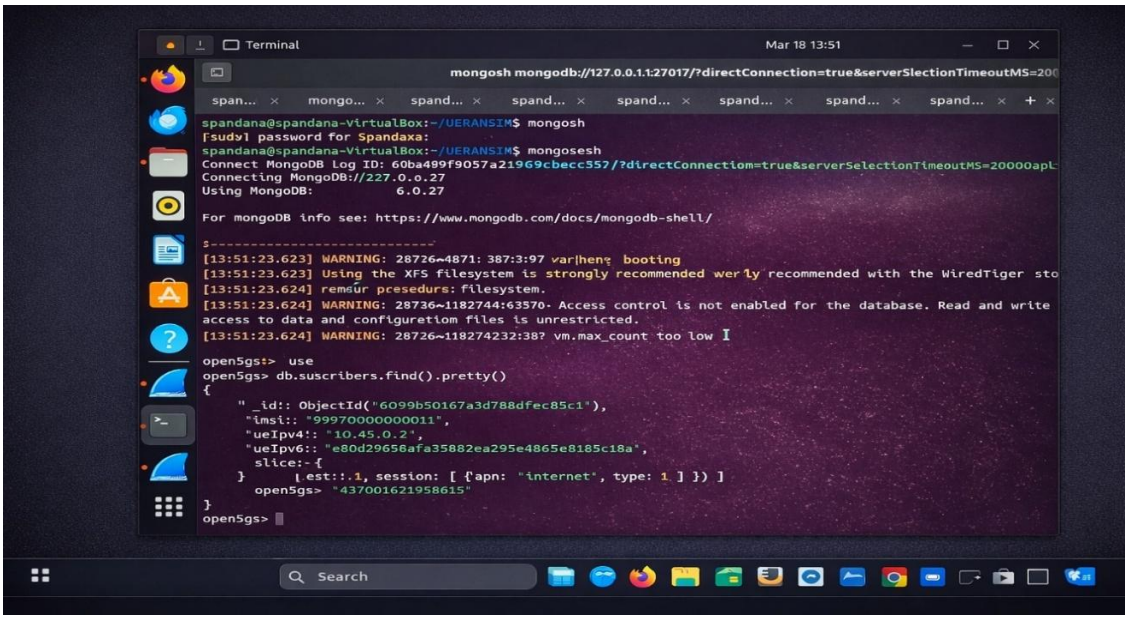

Fig 4.2: Terminal Output Displaying Access to MongoDB and Subscriber Information Retrieval.

The figure is the information of the subscriber obtained from the database. The existence of IMSI, authentication keys, session parameters is used to prove that the user equipment (UE) is properly registered and authenticated in the network

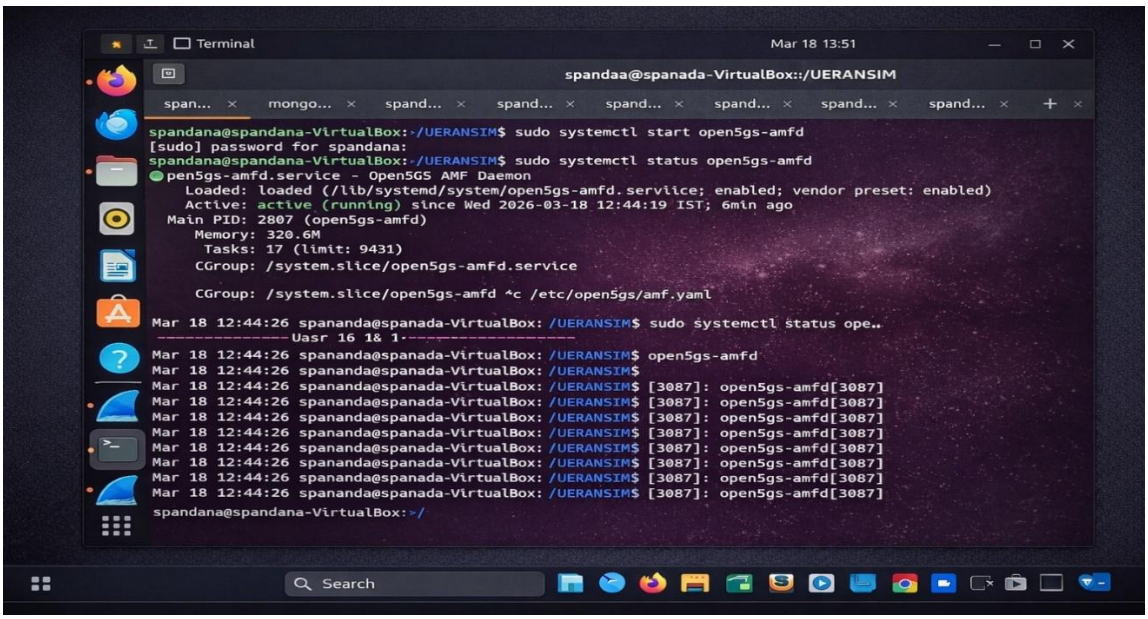

Fig 4.3: Terminal Output Demonstrating Successful Activation of AMF in 5G Core.

The AMF service status is used to show that the core network is up and ready to process signaling procedures between the UE and base station.

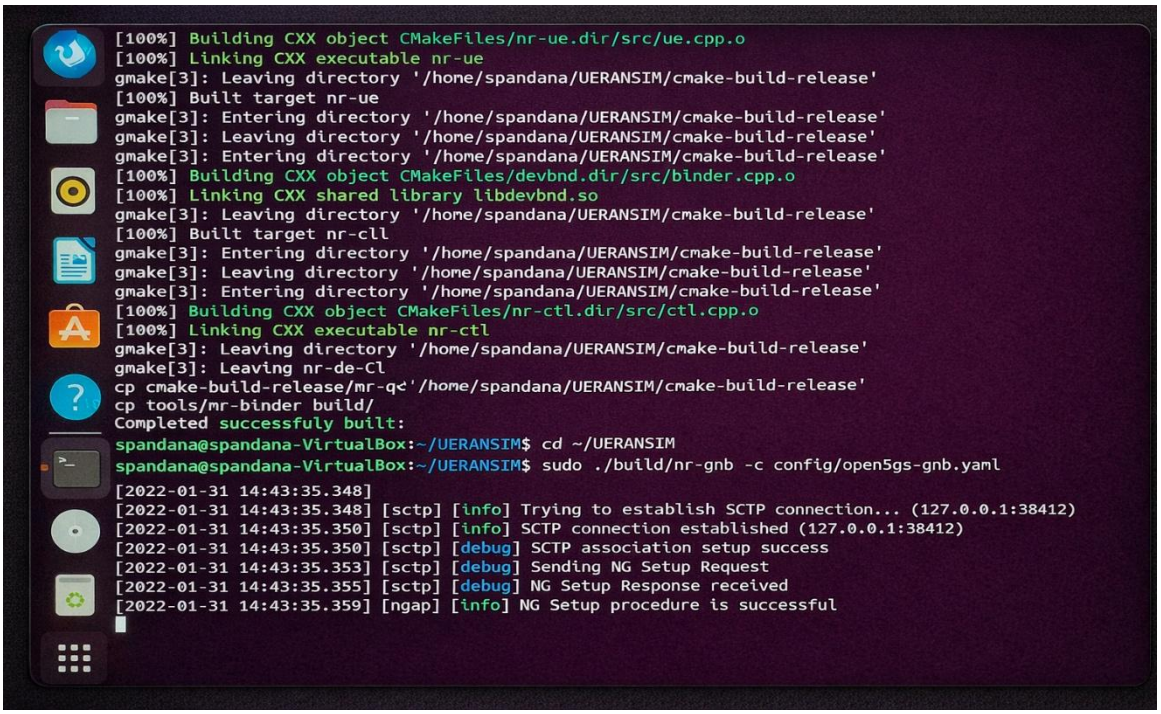

Fig 4.4: gNB Initializations and Successful Connection with 5G Core Network. The figure depicts the successful NG setup between gNB and 5G core network.

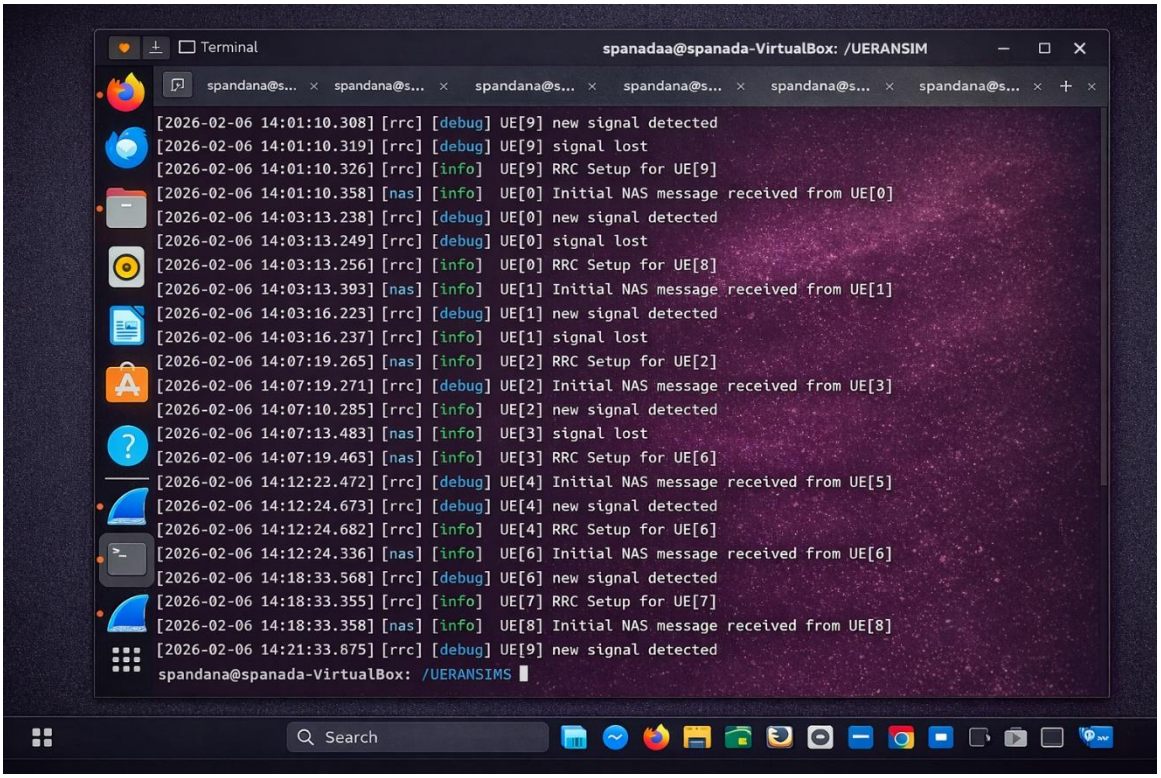

Fig 4.5: UE Activity Logs Showing Network Registration and Signal Events.

The logs of the UE terminal verify that the user terminal has successfully attached to the network and end-to-end connectivity has been established.

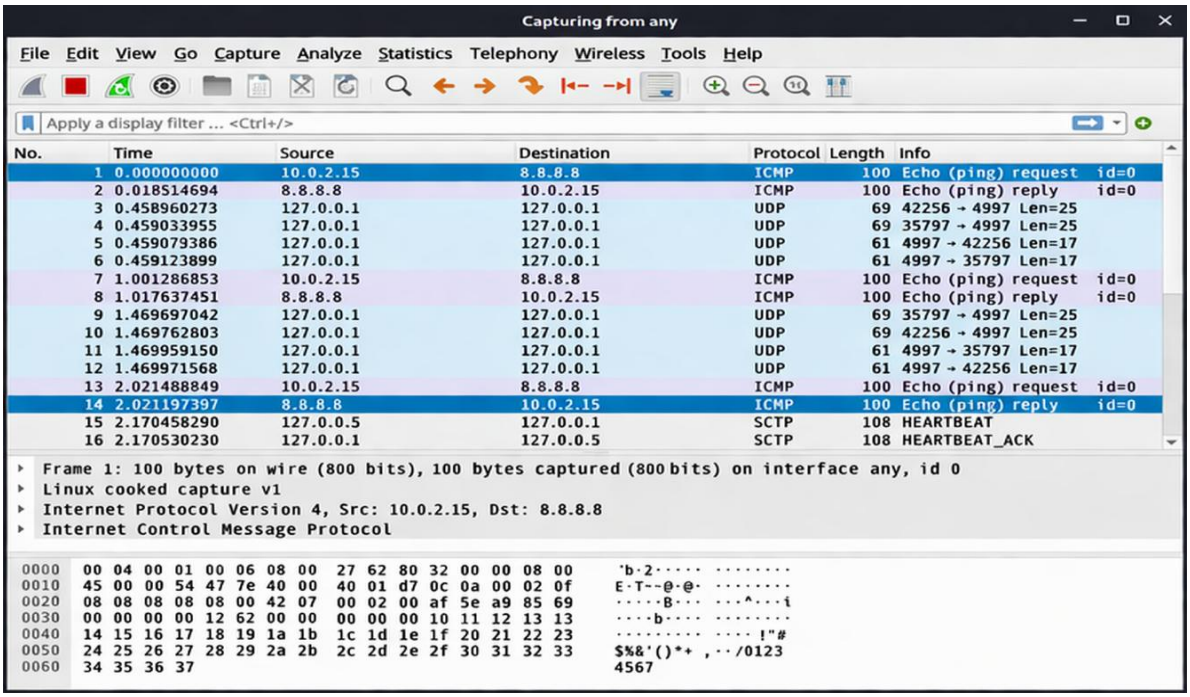

Fig 4.6 Wireshark Packet Capture Displaying Network Traffic and Protocol Analysis.

The captured packets contain signaling messages exchanged between the UE and network, which were used for the analysis of communication behavior and identification of anomalies.

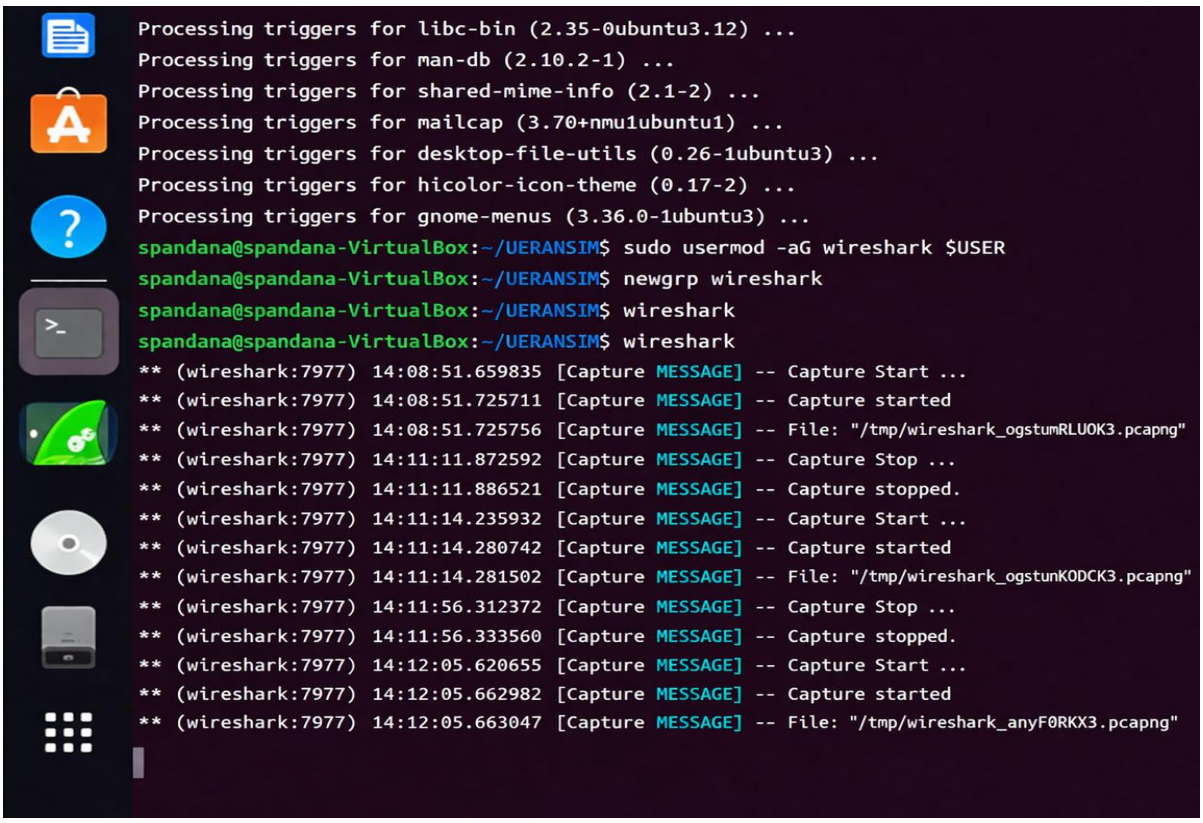

Fig 4.7: System Logs Indicating Packet Collection Activity and File Production.

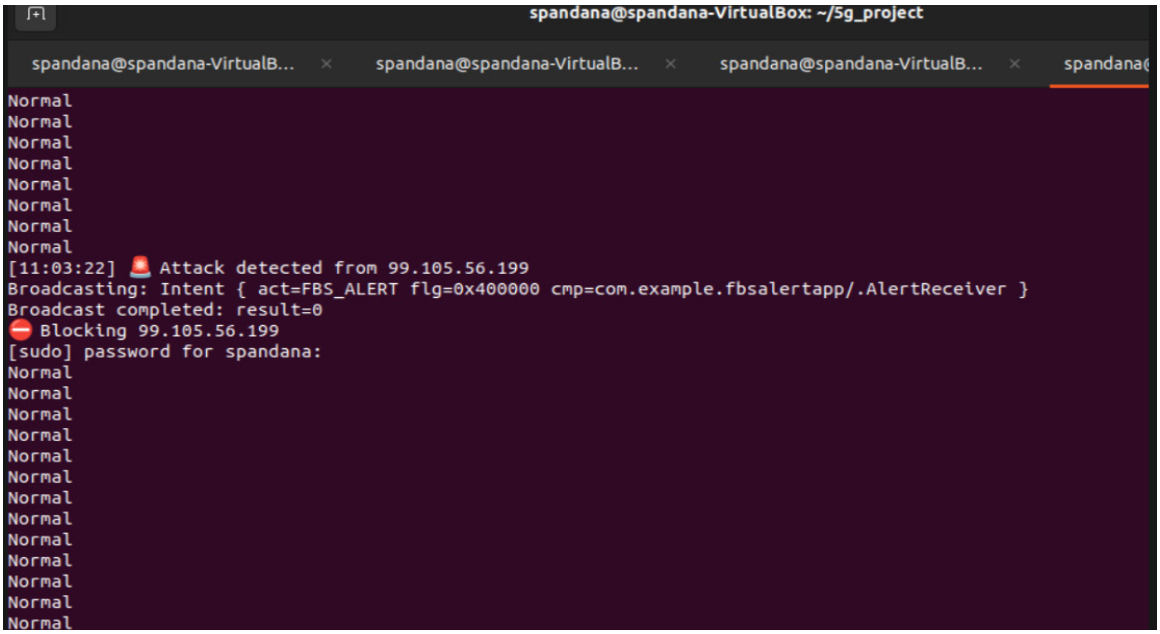

Fig 4.8: System Output Demonstrating the Detection of the Attack of a Fake Base Station and Mitigation of the Firewall. The figure shows the successful blocking of the suspicious IP address showing the capacity of the system to prevent further malicious communication.

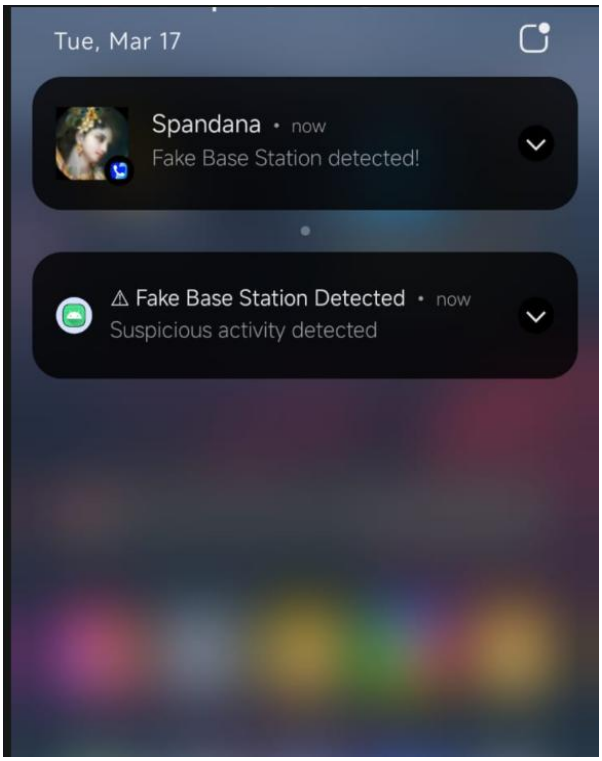

Fig 4.9: Mobile Alert Notification for Detected Activity of a Fake Base Station.

Overall, the results validate the feasibility of the proposed system for the detection and mitigation of fake base stations in real-time. The combination of machine learning and network-level controls provides both accuracy and an immediate response, making the system good for the deployment of 5G environments.

4.1 GRAPHS:-

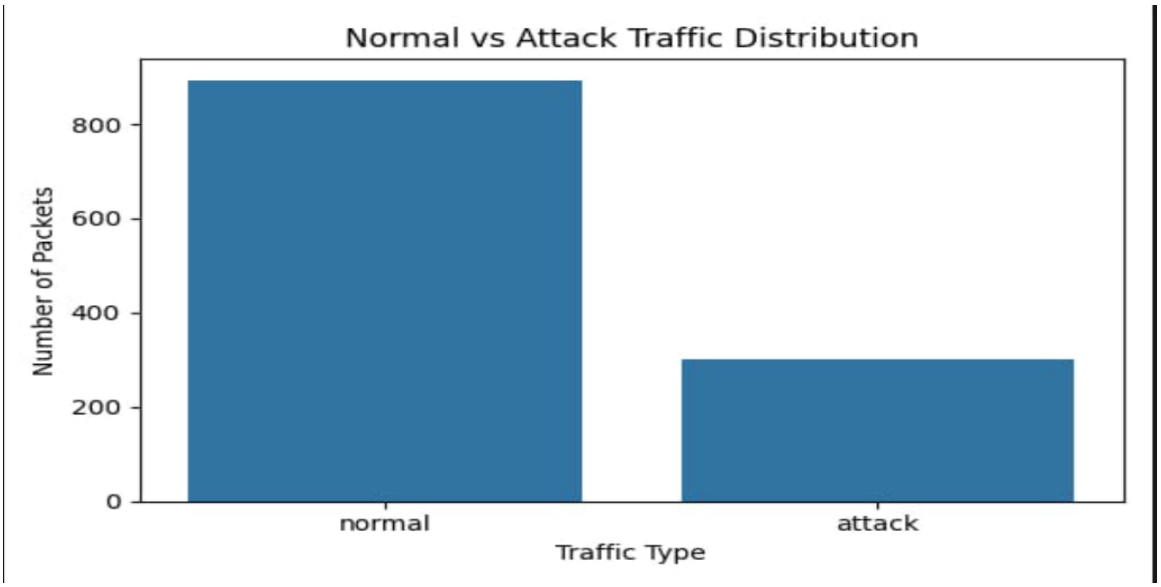

Fig 4.10: Comparison of Normal and Malicious Traffic with respect to the number of packets.

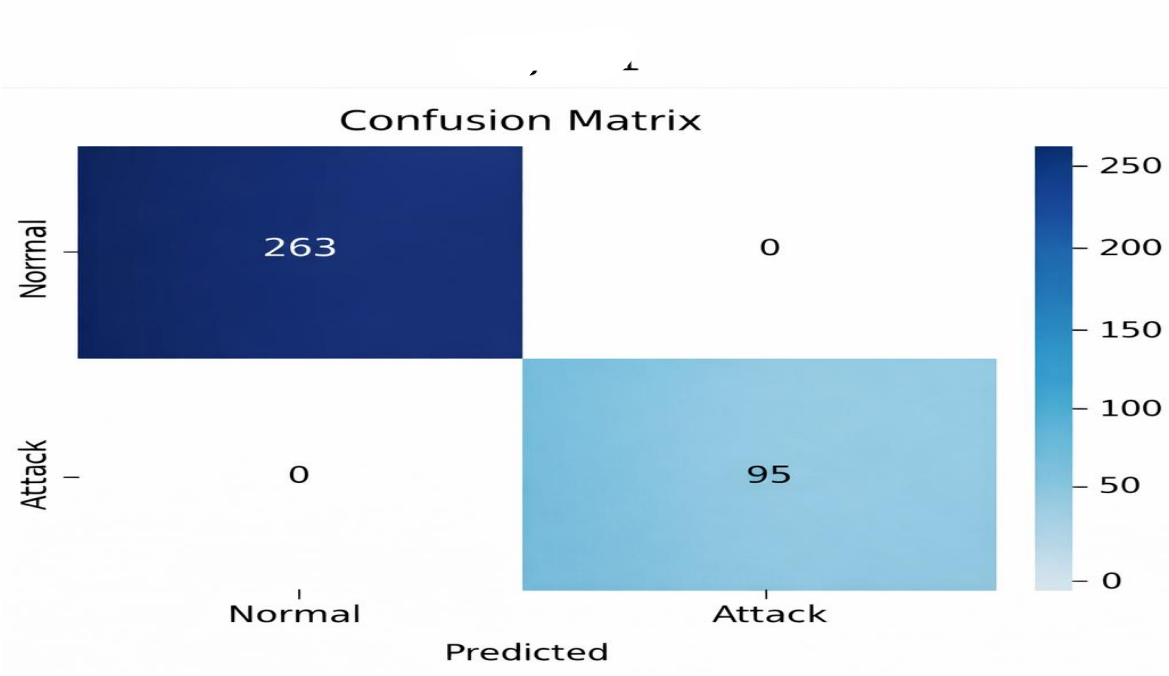

Fig 4.11: Accuracy of Normal vs Attack Detection Confusion Matrix.

Figure 4.10 and Figure 4.11 demonstrate the work of the proposed system regarding the identification of traffic and the accuracy of detection. It can be observed that the traffic distribution plot has a significant abundance of normal packets, some 900, when compared to other packets that were identified as attack packets and were correctly identified as about 300 packets, which also shows that differentiation between normal and malicious traffic was successful.

This confusion matrix also supports the performance of the model since there are no misclassifications, 263 normal instances and 95 attack instances were correctly classified. These outcomes are almost perfect, and this proves that the suggested system can be very dependable when it comes to identifying the presence of rogue operations of a base station. Not

having false positives and false negatives points to the strength with which the model can differentiate normal and malicious network behavior in real-time settings.

V. Conclusion

This paper proposes an overall outline of fake 5G base station detection and mitigation based on real-time monitoring, machine-learning-based fake 5G base station detection and automated mitigation strategies. Open5GS was successfully used to implement and evaluate the performance of that system in a controlled 5G environment with UERANSIM and in a realistic scenario. Findings suggest that the suggested method is a potential means of generating accurate results in terms of rogue base stations with minimal false positives and identification. In addition, the combination of mitigation measures that include IP blocking and the disconnection of user equipment is a measure that assures that the threats that are detected are not only identified but also neutralized. This is because the addition of user notification mechanisms in this work is a major contribution to the work that generates user awareness and provides an extra layer of security. The real-time nature of the system, combined with the high detection and response rate, makes it a viable tool in order to improve the security of contemporary 5G. Future research can focus on how to increase the scalability of the system, introduce powerful deep-learning-based models and expand the system to address more complicated attack cases with such systems deployed on large networks.

References

[1]. K. S. Mubasshir, I. Karim and E. Bertino, "Gotta Detect 'Em All: Fake Base Station and Multi-Step Attack Detection in Cellular Networks," in Proc. USENIX Security Symposium, 2025.

[2]. A. Islam et al., "Anomaly Detection Against Fake Base Station Threats in 4G/5G Networks," Electronics, vol. 5, no. 4, pp. 94, 2025.

[3]. S. Wuthier et al., "Fake Base Station Detection and Blacklisting," NSF Research Report, 2024.

[4]. M. Harvanek et al., "Survey on 5G Physical Layer Security Threats and Countermeasures," IEEE Access, 2024.

[5]. E. Yocam, 5G Mobile Networks: Security Control and Vulnerabilities. Springer, 2022.

[6]. A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani and E. Weippl, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," in Proc. 30th Annual Computer Security Applications Conference (ACSAC), 2014, pp. 246–255.

[7]. D. Wehrle, "Open Source IMSI Catcher," Master's thesis, Albert-Ludwig University of Freiburg, 2009.

[8]. J. Park and J. Kim, "Detection of Fake Base Stations Using Machine Learning Techniques," IEEE Access, vol. 8, pp. 123456–123468, 2020.

[9]. 3GPP, "Security Architecture and Procedures for 5G System," 3GPP TS 33.501, Release 16, 2020.

[10]. N. Golde, K. Redon, R. Borgaonkar, "Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications," in Proc. NDSS, 2012.

[11]. S. Hussain, O. Chowdhury, S. Mehnaz, E. Bertino, "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," in Proc. IEEE Symposium on Security and Privacy, 2018, pp. 446–462.

[12]. R. Bassil, A. Chehab, I. H. Elhajj, A. Kayssi, "Fake Base Station Detection in Cellular Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1234–1256, 2021.

[13]. N. M. Niranjan, "Detection, Prevention and Mitigation of Rogue Base Stations in 5G Networks," Technical Disclosure Commons, Mar. 2022. [Online]. Available: https://www.tdcommons.org/dpubs_series/4982.

[14]. A. Naveena and K. Pranathi, "FBMC Modulation Schemes for 5G Mobile Communications," Turkish Journal of Computer and Mathematics Education, vol. 12, no. 12, pp. 2520–2525, 2021.

[15]. K. P. Kumar and K. Pranathi, "A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability in case of Cyber Crime," JAC: A Journal of Composition Theory, vol. 14, no. 4, pp. 100–103, Apr. 2021.

[16]. K. Pranathi, FBMC Modulation Schemes for 5GMobile Communications, Turkish Journal of Computer and Mathematics Education, Vol. 12 no. 12 (2021), 2520–2525