S & M 4008

Rogue Base Station Detection in Industrial Internet of Things

I-Hsien Liu,[1,2] Hou-Hua Chen,[1,2] Bing-Han Tang,[1,2] and Jung-Shian Li[1,2*]

[1]Department of Electrical Engineering, National Cheng Kung University,
No. 1, University Road, Tainan City 701401, Taiwan
[2]Institute of Computer and Communication Engineering, National Cheng Kung University,
No. 1, University Road, Tainan City 701401, Taiwan

(Received August 5, 2024; accepted April 4, 2025)

Keywords: 5G, Industrial Internet of Things, base station, wireless security

The advent of 5G technology has markedly accelerated the development of the Industrial Internet of Things (IIoT), enabling faster and more reliable connectivity for various IoT devices. Many of these IIoT systems rely on sensor-based communication networks to monitor, collect, and transmit real-time data for industrial applications such as smart manufacturing, automated control systems, and predictive maintenance. However, this increased reliance on 5G networks introduces new cybersecurity risks, particularly the threat of rogue base stations that can intercept, manipulate, and disrupt data communications. In this study, we aim to identify and address the security threats posed by rogue base stations in the IIoT. Our detection approach is based on reference signal received power (RSRP) analysis, which allows us to monitor and evaluate signal strength variations. Since rogue base stations often transmit stronger signals to lure IIoT devices, abnormal fluctuations or inconsistencies in RSRP values can serve as key indicators of their presence. We use machine learning techniques, including recurrent neural networks, long short-term memory networks, and gated recurrent unit networks, to analyze and classify these signal patterns effectively. By leveraging the sequential nature of RSRP data, our model detects deviations from normal base station behavior, enabling the real-time identification of potential rogue base stations. By enhancing the security of sensor-driven IIoT systems, our approach ensures the protection of critical industrial operations that depend on real-time and accurate sensor data transmission.

1. Introduction

The rapid advancement of 5G technology has significantly accelerated the development of the Industrial Internet of Things (IIoT), providing fast and reliable connectivity for various IoT devices that are essential to modern industrial operations relative to 4th-generation mobile communication technology. These devices enhance monitoring, control, and automation across a range of sectors, including manufacturing, energy, transportation, and healthcare. They offer the potential for unprecedented efficiency, flexibility, and scalability. According to IoT Analytics, the IIoT market is expected to reach $145 billion by 2023, with a compound annual growth rate

[*] Corresponding author: e-mail: jsli@cans.ee.ncku.edu.tw

https://doi.org/10.18494/SAM5279

ISSN 0914-4935 © MYU K.K.
https://myukk.org/

of 17.9% projected through 2030.[1] Furthermore, there are currently over 8.4 billion connected devices globally, with projections indicating that this number will reach 75 billion by 2025.[2] This growth reflects the significant potential of IoT technologies and their profound impact across industries, enabling smart manufacturing, enhancing production efficiency, and boosting competitiveness.

However, the increased reliance on 5G networks introduces significant cybersecurity risks, particularly with the emergence of rogue base stations, also known as fake base stations or international mobile subscriber identity (IMSI) catchers. These malicious entities can impersonate legitimate base stations, intercepting, manipulating, and disrupting data communications between IIoT devices and their intended networks. Such attacks have the potential to result in a number of significant consequences for organizations, including unauthorized access to data, the loss of sensitive information, operational disruptions, and severe financial and reputational damage. As the IIoT rapidly develops, cybersecurity has become a paramount concern. The extensive connectivity of IIoT devices and systems offers considerable convenience but also introduces significant security risks. Many IIoT applications rely on real-time sensor data for industrial control, automated decision making, and predictive maintenance. If attackers infiltrate these networks, they can manipulate sensor data, leading to faulty automation, inaccurate monitoring, and even complete system failure. This could result in production downtime, safety hazards, and critical data breaches.

The large-scale data sharing inherent in IIoT operations gives rise to concerns regarding the protection of manufacturing data and intellectual property, which must be robustly safeguarded. Additionally, the interconnected global supply chains characteristic of the IIoT require comprehensive security measures to prevent supply chain attacks. Implementing encrypted communication, regular software updates, and compliance testing for IoT devices can enhance security and ensure stable operation in the IIoT environment. Given these challenges, there is an urgent need for advanced detection mechanisms to identify and mitigate the threats posed by rogue base stations, as traditional security measures often fall short in addressing these sophisticated attacks.

Several methodologies have been proposed to address the detection of rogue base stations. Lee *et al.*[3] explored the cybersecurity issues in 5G-enabled smart healthcare networks, focusing on the identification of rogue base stations and proposing targeted detection strategies to strengthen network defenses. Huang *et al.*[4] developed xApps for software-defined radio (SDR)-enabled Open Radio Access Network (O-RAN) systems, employing signal stability analysis and machine learning algorithms to identify rogue base stations. Saedi *et al.*[5] created realistic signal strength datasets by simulating 5G rogue base station scenarios, thereby enhancing the effectiveness of detection techniques. Additionally, Nakarmi *et al.*[6] applied machine learning to analyze reference signal received power (RSRP) characteristics, improving false base station detection accuracy. Liu *et al.*[7] proposed a comprehensive scheme to counter fake base stations in 5G-based smart healthcare networks, emphasizing the significance of robust mobile network security measures. Finally, Quintin[8] focused on the real-time identification of fake 4G LTE base stations, implementing advanced monitoring and alert mechanisms to promptly address threats.

The following section outlines the methodology employed in this study, including a detailed explanation of the rogue base station attack and the detection process. The subsequent section presents the experimental results, encompassing dataset preparation, performance evaluation, results, and discussion. Finally, the paper concludes with a summary of the key findings.

2. Methodology

2.1 Rogue base station attack

Rogue base stations pose significant security threats to the IIoT, as they have the potential to compromise data confidentiality, integrity, and availability. These malicious entities can perform unauthorized access and man-in-the-middle (MitM) attacks, thereby intercepting sensitive data such as operational parameters and industrial control commands. Rogue base stations exploit network protocol vulnerabilities to manipulate data, leading to incorrect device behavior and potential operational failures. Identity spoofing is another critical threat, whereby rogue base stations deceive devices into divulging sensitive information. Additionally, they can launch denial-of-service (DoS) attacks by overwhelming the network with traffic, disrupting normal operations, and degrading the trust and security of the IIoT environment. To investigate these threats, we designed an architectural framework to emulate rogue base station attacks in IIoT environments, demonstrating how these malicious activities can exploit system vulnerabilities. The detailed architecture designed for these attack simulations is shown in Fig. 1.

There are several steps involved in executing a rogue base station attack, as follows.

- Configuration of the Rogue Base Station: The initial phase of the attack entails the setup of the requisite hardware and software to establish a rogue base station. The attacker configures SDR and communication equipment to operate on specific frequencies and emulate the parameters of legitimate base stations, including cell ID, mobile network code (MNC), and mobile country code (MCC).

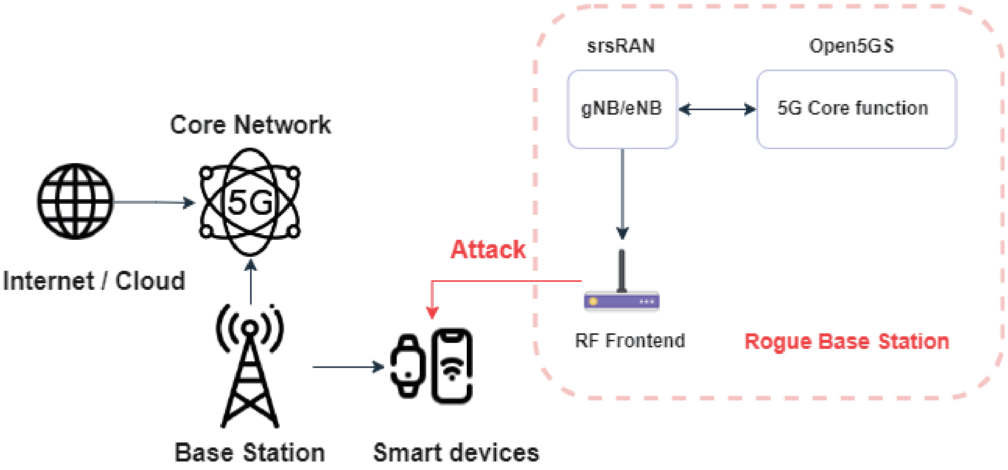

Fig. 1. (Color online) System architecture of rogue base station attacks.

- Positioning in the Target Area: After the setup phase is complete, the rogue base station is positioned in a way that allows it to effectively target the area in question. The attacker ensures that the signal strength of the rogue base station is greater than that of nearby legitimate base stations, thereby luring user devices into connecting to it. This often requires adjusting the location to optimize signal strength and effectively capture the devices in range.
- Launching Attacks: Once user devices connect to the rogue base station, the attacker can execute various malicious activities. These include intercepting and manipulating data communications, leading to the exposure of sensitive information. The attacker can also perform DoS attacks to disrupt services and MitM attacks to alter data traffic. Furthermore, fake messages such as service rejections, emergency alerts, or phishing messages can be sent to deceive users into revealing personal information or causing service disruptions.

A comparison between different parameters is shown in Table 1, and the detailed rogue base station attack process is shown in Fig. 2.

2.2 Detection process

To effectively detect rogue base stations in the IIoT, a structured detection process is implemented. This process involves the collection of signal data, the creation of a comprehensive

Table 1
Comparison between different parameters.

Parameter	Description	Example value (Global)
cell ID	Identifies a specific cell within a sector of a cellular network	186013
MNC	Identifies a mobile network operator within a country	01 (for some carriers)
MCC	Identifies the country of the mobile subscriber	310 (USA), 440-441 (Japan), 466 (Taiwan)

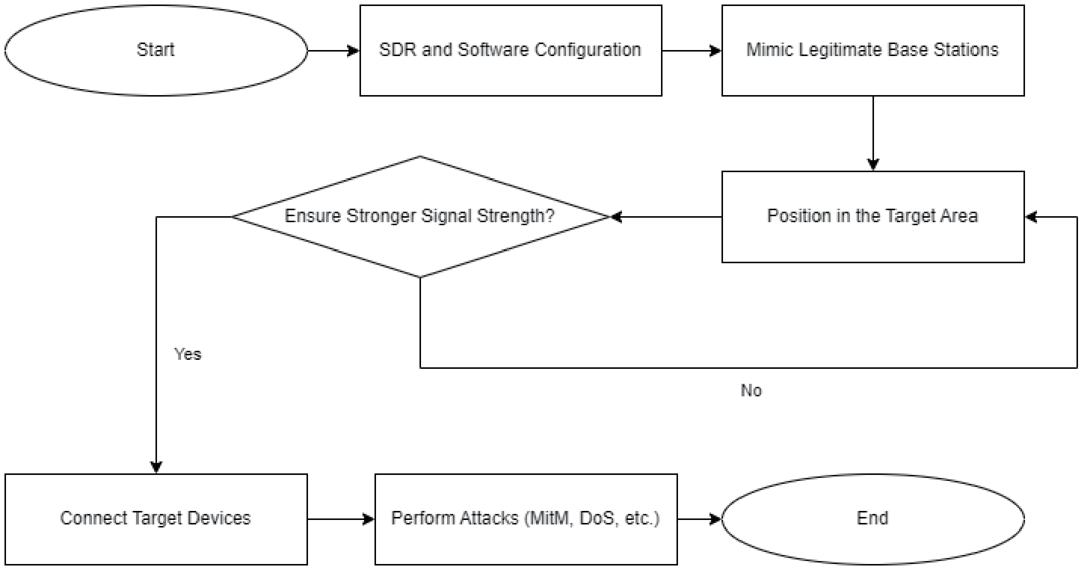
Start
SDR and Software Configuration
Mimic Legitimate Base Stations
Position in the Target Area
Ensure Stronger Signal Strength?
Yes
No
Connect Target Devices
Perform Attacks (MitM, DoS, etc.)
End

Fig. 2. Detailed rogue base station attack process.

dataset, and the application of advanced machine learning algorithms for classification and detection. The detailed rogue base station detection process is shown in Fig. 3.

The first step in this process is the collection of signal data from all detectable base stations in the environment. We employ SDRs to emulate the behavior of various IIoT devices and continuously gather data over various time intervals. This approach ensures the generation of a dataset that accounts for normal variations in signal strength. The collected data include parameters such as timestamp, cell ID, MNC, MCC, and signal strength values.

Once the data have been collected, it is aggregated into a dataset for subsequent analysis. From this dataset, relevant features are extracted, with a particular focus on the RSRP values. The RSRP is a crucial measure of the power level received by a device from a reference signal transmitted by a base station. This feature is selected for its reliability in indicating signal strength and can reveal significant variations that may indicate the presence of a rogue base station. Rogue base stations typically emit stronger RSRP signals to overpower legitimate base stations and lure user devices into connecting to them. Additional features such as average RSRP, signal strength variance, and temporal patterns of signal changes are also extracted. These features help in distinguishing between normal base station behavior and anomalies indicative of rogue base stations.

The dataset, which has been augmented with the extracted features, is labeled with both known legitimate base station information and potential rogue base station detections. The labeled dataset serves as the foundation for training advanced machine learning models, specifically recurrent neural network (RNN),(9) long short-term memory (LSTM),(10) and gated recurrent unit (GRU).(11) These models are particularly adept at handling sequential and time-series data,(12) which is essential for analyzing RSRP patterns over time.

By collecting and analyzing RSRP data using advanced machine learning techniques, the detection process aims to accurately identify rogue base stations in the IIoT, enhancing overall security and mitigating potential threats.

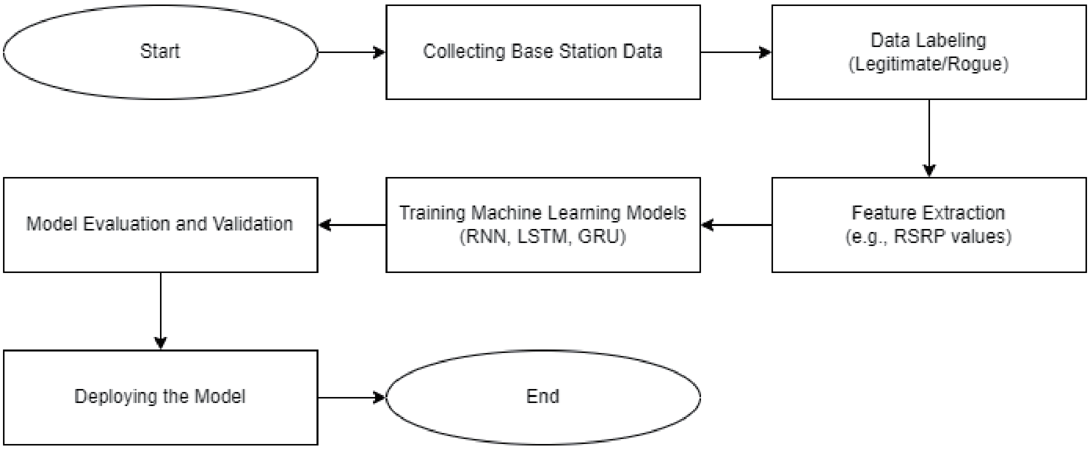

Fig. 3. Detailed rogue base station detection process.

3. Experimental Results

3.1 Dataset preparation

To investigate the issues of rogue base station attacks in the IIoT, we established a comprehensive framework that integrates specific hardware and software components designed for both legitimate and malicious activities. This configuration entails the deployment of two Universal Software Radio Peripheral (USRP) B210 devices, which are SDRs utilized for the flexible generation and reception of wireless signals.

A single USRP B210 is configured to emulate the 5G connection of an IIoT device. This device is set up to operate as a legitimate end-user device, interacting with the network in a manner consistent with that of a typical IIoT device. The transmission parameters are adjusted to ensure an accurate representation of real IIoT device communication.

The second USRP B210 is configured to operate as a rogue base station.(13) This device is specially set up to imitate a legitimate base station by adjusting its transmission parameters to match those used in real networks. This allows it to deceive user devices into connecting to it instead of a legitimate base station.

srsRAN(14) is utilized for the configuration of the rogue base station, whereby network parameters such as cell ID, MNC, and MCC are set. These parameters must be identical to those of a legitimate base station to deceive user devices into connecting to the rogue base station. Additionally, Open5GS(15) is employed to establish the core network functions of the rogue base station, including the management of subscriber data, session management, and other critical network services that are necessary for a fully functional rogue setup.

The data collection process begins by configuring the USRP B210s to operate on the desired frequency bands. The initial USRP B210 emulates IIoT device communication and collects data to create a dataset for subsequent detection processes. The second USRP B210's transmission settings are adjusted to ensure the accurate mimicry of a legitimate base station. Next, srsRAN is configured to define the network parameters (cell ID, MNC, and MCC) to match those of a real base station.

This dataset is then used for machine-learning-based classification, where RNNs, LSTM networks, and GRU networks analyze the temporal variations in RSRP values to effectively identify rogue base stations. The results demonstrate that our method successfully detects rogue base stations by leveraging RSRP-based time-series analysis, providing a highly accurate and adaptive security mechanism for IIoT environments.

3.2 Performance evaluation

To address the security risks posed by rogue base stations in the IIoT, we implemented a robust detection process utilizing advanced machine learning algorithms. The primary focus is on the analysis of RSRP values, with the objective of identifying anomalies indicative of rogue base stations.

Three advanced machine learning models were employed in this investigation. The models utilized in this study were RNN, LSTM, and GRU. These models are particularly well suited for handling sequential and time-series data, making them ideal for the analysis of RSRP patterns over time. The RNN model processed sequences of RSRP data, identifying patterns and anomalies based on historical data and capturing the immediate signal variations indicative of rogue activity. The LSTM model captured long-term dependences in the RSRP data, detecting gradual changes in signal patterns. The GRU model, being a variant of the LSTM model, enabled the efficient and effective modeling of the RSRP data, balancing performance and computational efficiency.

In our performance evaluation, we focused on four key metrics: precision, recall, F1 score, and true-negative rate (TNR).[12] These metrics were selected for their ability to provide a comprehensive assessment of the effectiveness of each model in detecting rogue base stations.

3.3 Results

In this study, we employed a dataset comprising a total of 1000 data points, with an equal distribution of 500 data points for legitimate base stations and 500 data points for malicious base stations. The data set was split into training and testing sets, with 80% of the data used for training and 20% for testing.

The experiment results are shown in Table 2. The LSTM model achieved the highest TNR of 0.9712, demonstrating its effectiveness in distinguishing between legitimate and rogue base stations. The GRU model also performed well, with a high F1 score of 0.9691 and a TNR of 0.9615. The RNN model, while still effective, showed the lowest performance among the three models, particularly in terms of TNR, which was 0.9327.

Analyzing the number of parameters, we observed that the LSTM model has the highest parameter count at 4385, followed by the GRU model with 3393 parameters, and the RNN model with 1121 parameters. This indicates that the LSTM and GRU models, despite having more parameters, can achieve higher performance metrics. The enhanced complexity of these models contributes to their superior capacity to detect rogue base stations in the IIoT environment, emphasizing the trade-off between model complexity and detection.

3.4 Discussion

The experimental results demonstrate that all three neural network models (RNN, LSTM, and GRU) performed exceptionally well in detecting rogue base stations in the IIoT environment. Each model exhibited high precision, recall, F1 score, and TNR, with all metrics exceeding 0.9,

Table 2
Comparison between different peer methods.

Method	Precision	Recall	F1 score	TNR	Parameter
Simple RNN	0.9314	**0.9896**	0.9596	0.9327	1121
LSTM	**0.9684**	0.9583	0.9634	**0.9712**	4385
GRU	0.9592	0.9792	**0.9691**	0.9615	3393

Table 3
Comparison of rogue base station detection methods.

Feature	Huang *et al.*(4)	Nakarmi *et al.*(6)	Liu *et al.*(7)	Proposed method
RSRP characteristic	✓	✓		✓
Machine learning	✓	✓		✓
Using SDR	✓		✓	✓
High precision	✓	✓	✓	✓

indicating their robustness and reliability in distinguishing between legitimate and malicious base stations.

The LSTM model was particularly effective, achieving the highest performance among the three models. The GRU model also showed strong performance, closely following the LSTM model. The RNN model was slightly less effective but still provided reliable detection capabilities. These results highlight the potential of advanced machine learning models to enhance the security of IIoT networks by accurately identifying rogue base stations.

To better understand how our approach compares to existing methods for detecting rogue base stations, we evaluated key features of previous studies. Table 3 provides a comparative summary of these methods. While previous works successfully leveraged RSRP characteristics and machine-learning-based detection, our proposed method differs by integrating both techniques with SDR emulation. This combination enables a more flexible and adaptable detection mechanism, especially in IIoT environments where rogue base stations take advantage of dynamic network conditions. Furthermore, our models consistently achieve high accuracy, matching the best performing previous works, while demonstrating superior adaptability through time-series analysis.

Our method integrates machine learning with time-series analysis, offering significant advantages over previous approaches. By emulating IIoT environments using SDR, our system effectively detects rogue base stations through temporal signal variations, ensuring dynamic detection capabilities while maintaining ease of deployment across various devices. Compared with traditional methods, our approach provides higher accuracy, improved adaptability, and enhanced security, making it a robust and scalable solution for safeguarding IIoT environments against rogue base station threats.

4. Conclusions

In this study, we designed a framework to emulate a rogue base station attack and collected data to represent both legitimate and malicious base station scenarios. Three advanced machine learning models (RNN, LSTM, and GRU) were used to classify and detect rogue base stations based on RSRP values. Each model demonstrated high performance, with all key metrics exceeding 0.9. While our proposed method enhances the security of IIoT networks by enabling the real-time detection of rogue base stations, several challenges remain. A key limitation is the reliance on RSRP values alone, which can be affected by environmental factors such as interference, signal reflections, and obstacles. Future work can incorporate an additional wireless signal parameter, such as reference signal received quality or signal-to-interference-plus-noise ratio, to improve detection robustness. In addition, expanding the dataset to include real-world deployment scenarios and testing in different IIoT environments will improve the generalizability of the model. In addition, the integration of edge computing solutions can enable the faster and real-time detection of rogue base stations at the network edge, reducing reliance on centralized infrastructure. By addressing these challenges, our research lays the foundation for a more secure and resilient IIoT ecosystem, ensuring reliable communications and protecting industrial networks from rogue base station threats.

Acknowledgments

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract numbers NSTC 113-2221-E-006-147-MY2 and NSTC 113-2634-F-006-001-MBK.

References

1 Industry 4.0 check-in: 5 learnings from ongoing digital transformation initiatives: https://iot-analytics.com/industry-4-0-check-in-5-learnings-from-digital-transformation-initiatives/ (accessed July 2024).

2 X. Chen, D. W. K. Ng, W. Yu, E. G. Larsson, N. Al-Dhahir, and R. Schober: IEEE J. Sel. Areas Commun. **39** (2021) 615. https://doi.org/10.1109/JSAC.2020.3019724

3 M. H. Lee, I. H. Liu, H. C. Huang, and J. S. Li: Eng. Proc. **55** (2023) 50. https://doi.org/10.3390/engproc2023055050

4 J. H. Huang, S. M. Cheng, R. Kaliski, and C. F. Hung: Proc. 2023 IEEE INFOCOM - IEEE Conf. Computer Communications Workshops 3. (IEEE, 2023) 1.

5 M. Saedi, A. Moore, P. Perry, M. Shojafar, H. Ullah, and J. Synnott: Proc. 2020 IEEE Conf. Communications and Network Security (IEEE, 2020) 1.

6 P. K. Nakarmi, J. Sternby, and I. Ullah: Proc. 17th Inter. Conf. Availability, Reliability and Security (ACM, 2022) 60.

7 I. H. Liu, M. H. Lee, H. C. Huang, and J. S. Li: Appl. Sci. **13** (2023) 11565. https://doi.org/10.3390/app132011565

8 Detecting Fake 4G LTE Base Stations in Real Time: https://www.usenix.org/conference/enigma2021/presentation/quintin (accessed July 2024).

9 D. E. Rumelhart, G. E. Hinton, and R. J. Williams: Nature **323** (1986) 533. https://doi.org/10.1038/323533a0

10 S. Hochreiter and J. Schmidhuber: Neural Comput. **9** (1997) 1735. https://doi.org/10.1162/neco.1997.9.8.1735

11 K. Cho, B. van Merrienboer, C. Gulcehre, D. Bahdanau, F. Bougares, H. Schwenk, and Yoshua Bengio: arXiv (2014). https://doi.org/10.48550/arXiv.1406.1078 (accessed July 2024).

12 F. M. Shiri, T. Perumal, N. Mustapha, and R. Mohamed: arXiv (2023). https://doi.org/10.48550/arXiv.2305.17473 (accessed July 2024).

13 3rd Generation Partnership Project: Study on 5G Security Enhancement: https://www.3gpp.org/ftp/Specs/archive/33_series/33.809/ (accessed July 2024).

14 srsRAN Project: https://www.srslte.com/ (accessed July 2024).

15 Open5GS: https://open5gs.org/ (accessed July 2024).