


# Field Measurement Results on the Presence of Rogue Base Stations (Fake BTS) in Urban Areas

Mahadi Pardede

Universitas Pendidikan Indonesia

Article Info	ABSTRACT
<p><b>Article history:</b></p> <p>Received April, 2025 Revised April, 2025 Accepted April, 2025</p> <hr/> <p><b>Keywords:</b></p> <p>Rogue Base Station Fake BTS Detection Cellular Network Security Signal Anomaly Analysis Spectrum Monitoring</p>	<p>This research examines the presence and technical characteristics of rogue base stations (illicit BTS) through empirical field assessments conducted in densely populated urban environments. By employing a spectrum analyzer alongside the G-NetTrack application across frequency ranges extending from 900 to 2300 MHz, the investigation revealed signal anomalies that are suggestive of unauthorized base station operations. The signals that were detected displayed abnormal intensities coupled with variable stability, abrupt shifts from 4G/5G networks to 2G networks, and discrepancies in cell ID and network identity parameters (MCC, MNC, LAC). These attributes imply coerced connections to illegitimate transmitters. The rogue BTS units were predominantly located in close proximity to governmental offices, commercial hubs, and public venues, thereby indicating a potentially strategic deployment approach. The results underscore the critical necessity for the implementation of early detection systems and inter-agency cooperation to alleviate the risks associated with communication interception. By furnishing technical indicators and empirical measurement data, this study contributes to the advancement of network security frameworks and informs policy formulation aimed at safeguarding cellular infrastructure.</p> <p><i>This is an open access article under the <a href="#">CC BY-SA</a> license.</i></p> <div></div>

**Corresponding Author:**

Name: Mahadi Pardede  
Institution: Universitas Pendidikan Indonesia  
Email: [adipardede@upi.edu](mailto:adipardede@upi.edu)

**1. INTRODUCTION**

The rapid evolution of mobile technology has significantly altered the methodologies through which individuals partake in communication, acquire information, and conduct digital transactions. In light of the pervasive adoption of mobile phones, cellular networks have emerged as a critical pillar of digital infrastructure, facilitating a diverse array of activities encompassing economic transactions, social interactions, and governmental operations

(ITU, 2021). In the Indonesian context, the importance of mobile networks is particularly accentuated, especially within sectors such as banking services, public utilities, and frameworks of national security. As a result, the protection of these networks extends beyond mere technical concerns; it is essential for safeguarding personal data, privacy rights, and the digital sovereignty of the nation (Zhou et al., 2019; Nguyen, Lin, & Li, 2021; Rysavy, 2019; Asokan et al., 2022).

However, as the critical nature of these networks has escalated, their

vulnerability to various threats has simultaneously increased. One of the most concerning developments is the rise of illicit surveillance devices, such as rogue base stations (RBS), informally known as fake BTS. These devices allow unauthorized actors to impersonate legitimate base stations, thereby intercepting user communications without detection. The seriousness of this threat is compounded by the reality that average users typically lack the ability to identify any anomalies, as there are no overt signs indicating that their devices have connected to a fraudulent BTS (Shaik et al., 2015; Hussain et al., 2021; Borgaonkar, Redon, & Seifert, 2014). From a national security standpoint, fake BTSs may be leveraged for activities such as espionage, data theft, information manipulation, and the disruption of strategic communications (Arik & Poznanski, 2016; Abdalla & Tariq, 2023; Hoang & Nguyen, 2023).

Unfortunately, existing detection mechanisms remain insufficient, and the technical oversight of base station infrastructure is marked by significant deficiencies. Moreover, regulatory frameworks have yet to fully adapt to the unique security challenges introduced by these rogue devices. This predicament results in a considerable vulnerability within Indonesia's digital defense system. Addressing this issue cannot rest solely with telecom operators; it requires a collaborative effort from regulators, law enforcement agencies, researchers, and stakeholders in the technology sector (Rupprecht et al., 2018; Karim, Fatima, & Shah, 2022; Ismail & Ahmad, 2021; Adepu & Mathur, 2018).

Fake BTSs present a formidable threat. They possess the ability to replicate legitimate signals, trick devices into forming connections with them, and subsequently intercept or manipulate communications. Some of these devices are designed to track users' locations in real-time, disrupting access to authentic networks (thereby creating denial-of-service situations), or injecting malicious content such as malware or phishing links (Park et al., 2020; Dabrowski et

al., 2014; Rupprecht et al., 2018; Zhang, Lin, & Shen, 2019; Liu et al., 2015). In certain cases, these devices have been exploited by state actors for espionage activities (Marzouki et al., 2021; Han, Wu, & Wang, 2022; Liu, Yang, & Shen, 2019).

Despite the inherent risks, there is a significant lack of empirical investigation regarding the operational environments and prevalence of counterfeit base transceiver stations (BTSs). A considerable portion of the existing knowledge remains predominantly theoretical or extrapolated from simulations, primarily attributable to the difficulties in obtaining genuine incident data. Operators often demonstrate hesitance in disclosing such events, and the technological tools necessary for identifying these illicit devices are not consistently available or user-friendly (Lanz et al., 2020; Kim, Lee, & Park, 2022; Lashkari et al., 2020; Letaief et al., 2019). This dearth of authentic data hinders the development of effective policies or technical solutions. Consequently, empirical field studies are critically needed to obtain an accurate, practical, and contextually nuanced understanding of the growing threat posed by illicit base stations.

## 2. LITERATURE REVIEW

### 2.1 *Understanding Base Stations and Rogue BTS*

A Base Transceiver Station (BTS) constitutes a fundamental component within the cellular network architecture, serving as the intermediary between mobile devices and the core network operated by telecommunications providers. It is responsible for managing radio communications, overseeing frequency channel allocations, and facilitating cell handover operations. Authorized BTS units' function under the auspices of licensed mobile operators and are subject to regulation by national telecommunications authorities (Pemerintah Republik Indonesia, 1999).

Conversely, a rogue base station (RBS)—commonly referred to as a counterfeit BTS—represents an unauthorized apparatus that

replicates the functionalities of a legitimate BTS for nefarious objectives, including the interception of communications or the illicit collection of personal data (Shaik et al., 2015: 4). These fraudulent units attract proximal mobile devices by emitting signals of greater strength than those produced by legitimate BTSs, thereby exploiting weaknesses inherent in cellular authentication protocols (Rupprecht et al., 2018: 112). They have been employed in a variety of scenarios, ranging from cybercrime and surveillance to political espionage (Marzouki et al., 2021: 89).

## **2.2 Second Previous Research on Fake BTS and Network Anomalies**

A burgeoning corpus of scholarly research has scrutinized the perils associated with malevolent Base Transceiver Stations (BTS). For example, Dabrowski et al. (2014) illustrated the capacity of these devices to intercept both voice and data communications, as well as to monitor a user's geographical position in real-time. Zhou et al. (2019: 57) underscored that such threats are particularly perilous for susceptible populations including journalists, activists, and public officials. Arik and Poznanski (2016) elaborated further, noting that the efficacy of counterfeit BTS attacks is primarily attributable to the inadequacies of authentication protocols within mobile telecommunications networks.

In response to these challenges, researchers have investigated a variety of detection methodologies and instruments, including software-defined radios (SDRs), IMSI catchers, and signal scanning applications such as AIMSICD, CellMapper, and G-NetTrack (Hussain et al., 2021). These instruments are predicated on technical parameters—namely, Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), Cell ID, and signal strength—to identify anomalous or suspicious signal behavior (Dabrowski et al., 2014).

Notwithstanding the heightened awareness surrounding these issues, empirical field investigations remain scarce. Lanz et al. (2020) highlighted that limited

access to authentic incident data and a dearth of reporting from mobile network operators have obstructed substantive research efforts. Consequently, numerous proposed detection methodologies tend to be either theoretical or simulation-based, rather than grounded in empirical field conditions (Kim, Lee, & Park, 2022).

## **2.3 Theoretical Frameworks for Detection**

Two principal theoretical frameworks underpin the identification of illicit Base Transceiver Stations (BTS). The initial framework is spectrum surveillance, which operates on the premise that all radio communications must adhere to authorized frequency allocations. Any transmission manifesting outside of designated bands may be categorized as unlawful (Pemerintah Republik Indonesia, 1999). This paradigm depends on real-time monitoring mechanisms and official frequency registries to discern aberrations.

The subsequent framework is the intrusion detection paradigm pertinent to mobile telecommunications networks. This methodology encompasses four fundamental phases: data acquisition of signals, analysis of behaviors, recognition of anomalies, and implementation of corrective measures (Abdalla & Tariq, 2023). A particularly efficacious strategy within this framework is the observation of "handover reject" incidents (for instance, code cc11), which signify unsuccessful connection endeavors attributable to unrecognized or invalid base stations.

When these two methodologies are integrated, they yield a robust framework for preemptive detection—capturing both atypical signal intensity and anomalous network behavior. Furthermore, they facilitate the advancement of artificial intelligence-enhanced detection systems that can adjust to empirical conditions by leveraging field data and fostering inter-operator collaboration (Park et al., 2020).

### 3. METHODS

This investigation employs a descriptive-exploratory research methodology, with the objective of capturing and analyzing empirical data regarding the occurrence and conduct of rogue base stations (illicit BTS) within urban settings. The descriptive component facilitates a nuanced representation of the intricate technical characteristics of signal behavior, whereas the exploratory facet enables researchers to identify novel patterns and risks that may have previously eluded documentation. This methodological approach is particularly apt for examining threats such as counterfeit BTS, which typically function in a clandestine manner and are infrequently reported.

The primary focus of this inquiry is the technical signal anomalies that may signify the operation of rogue base stations. These anomalies encompass irregular signal strength, abrupt alterations in network identification codes, and atypical transitions among network types (for instance, shifting from 4G or 5G to 2G). Concurrently, the subjects of the investigation are the diverse cellular signals detected across the designated research locale.

The research was executed in Jakarta, the capital of Indonesia and one of its most densely interconnected cities. Jakarta was selected due to its strategic significance as a national center for governmental operations, financial institutions, and digital communications. These elements render it a probable target for unauthorized surveillance endeavors. Although the precise dates of the study were not delineated, data collection occurred across a spectrum of locations within the city that were identified as high-risk or high-traffic zones.

To gather empirical data, the research team utilized two principal instruments. Initially, a spectrum analyzer was employed to scan and monitor the radio frequency spectrum, thereby facilitating the detection of any unauthorized transmissions. Subsequently, the G-NetTrack mobile application was installed on an Android

device to log technical signal parameters, which include signal strength (RSRP), signal quality (RSRQ), cell identity codes (Cell ID, LAC), and GPS coordinates. This amalgamation of tools provided a comprehensive overview—both from a broader frequency perspective and from the vantage point of a typical mobile device's experience.

While no formal sampling framework was delineated, the study adopted a purposive sampling strategy, intentionally concentrating on strategic urban locales where rogue BTS units would likely exert their efficacy—such as in proximity to governmental edifices, commercial districts, and public facilities. Data collection involved the real-time monitoring of signal activity at these sites and the documentation of any suspicious patterns or anomalies. Field observations were particularly attentive to signal behavior that diverged from anticipated norms, such as inconsistent signal strength, swiftly fluctuating BTS identifiers, and network downgrades that limited users to emergency call functionalities exclusively.

The amassed data underwent analysis utilizing a comparative and inferential methodology. Recorded signals were juxtaposed against baseline parameters derived from recognized, legitimate base stations. A multivariate model was employed to classify potential threats: if a signal exhibited more than four out of six critical technical anomalies, it was flagged as a probable rogue base station. These indicators encompassed irregular RSRP/RSRQ values, discrepancies in network identity, and evidence of enforced downgrades. This straightforward yet efficacious framework functions as an early detection system that, with further refinement, could evolve into an automated threat detection solution underpinned by machine learning methodologies.

### 4. RESULTS AND DISCUSSION

The findings of this investigation unequivocally demonstrate the existence of

rogue base stations (illegitimate BTS) across multiple urban locales in Jakarta, identified through direct empirical measurements utilizing both spectrum analyzers and the G-NetTrack application. The information collected unveiled signals exhibiting anomalous characteristics that significantly diverge from the norms associated with authentic cellular base stations. These anomalies encompass abnormally elevated signal strengths (ranging from  $-60$  to  $-70$  dBm), erratic network identifiers (notably fluctuating Cell ID and LAC), and recurrent forced transitions from 4G or 5G networks to 2G. This regression frequently resulted in devices manifesting an “emergency calls only” status or led to recurrent call drops—indicators that strongly imply unauthorized and potentially deleterious network interference.

Further scrutiny revealed that these irregularities were not randomly dispersed but were predominantly situated in proximity to pivotal locations, including government edifices, business districts, and public venues characterized by substantial communication traffic. This spatial distribution corroborates the hypothesis that rogue BTS units are strategically deployed—targeting high-value communication zones, ostensibly for purposes of interception, surveillance, or data expropriation.

Table 1 systematically contrasts the characteristics of signals originating from legitimate versus rogue BTS sources, accentuating distinct disparities in signal strength, stability, and network identifiers. Figures 1 through 8 present spectrum visualizations across various frequencies (900 MHz, 1800 MHz, 2100 MHz, 2300 MHz), elucidating the divergence between normative and suspect signals. Notably, rogue BTS signals exhibit pronounced peaks and erratic waveforms, in stark contrast to the smoother, more consistent profiles observed in sanctioned transmissions.

In juxtaposition with prior investigations, the outcomes of this research substantiate existing literature concerning rogue BTS behaviors. For example, Shaik et al.

(2015) and Rupprecht et al. (2018) identified analogous signal anomalies, including robust yet unstable signals and atypical network downgrades. However, this study enriches the discourse by providing empirical field data from an Indonesian urban setting, which has been comparatively underrepresented in the prevailing literature. Furthermore, the patterns discerned in Jakarta correspond with the strategic deployment behaviors delineated by Marzouki et al. (2021), indicating a calculated exploitation of densely populated communication zones.

The research also introduces a preliminary multivariate detection model, wherein signals that fulfill at least four out of six anomalous criteria are flagged as potentially detrimental. This model establishes a foundational framework for the prospective development of automated early warning systems, particularly if integrated with machine learning algorithms trained on an expanding dataset of signal anomalies.

In summary, the findings substantiate the central research inquiry regarding the technical characteristics and spatial distribution of rogue BTS units. The analysis accentuates the pressing necessity for enhanced regulatory frameworks, real-time spectrum monitoring systems, and intersectoral collaboration among telecommunications operators, regulators, and law enforcement to alleviate this threat. These findings serve as both a technical reference and a policy foundation for fortifying cellular network security in Indonesia.

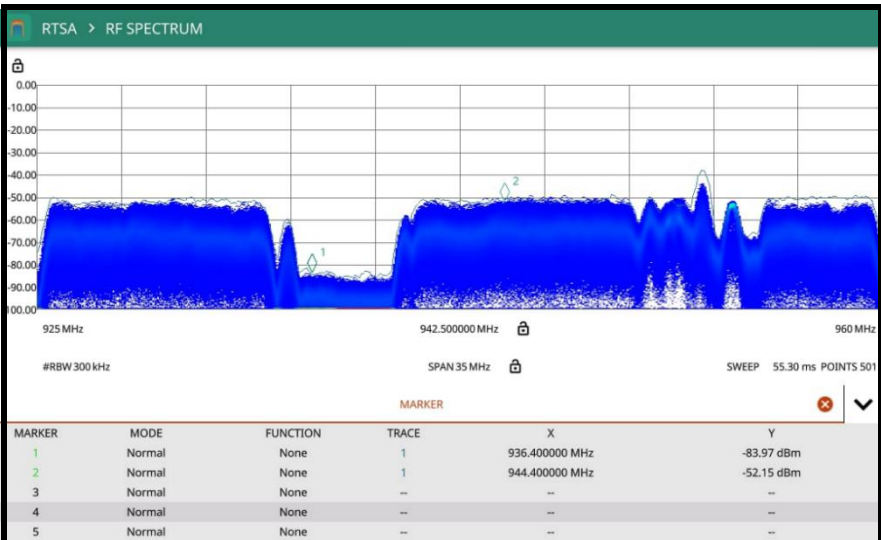


Figure.1. Measured results of 900 MHz radio frequency of the Official BTS

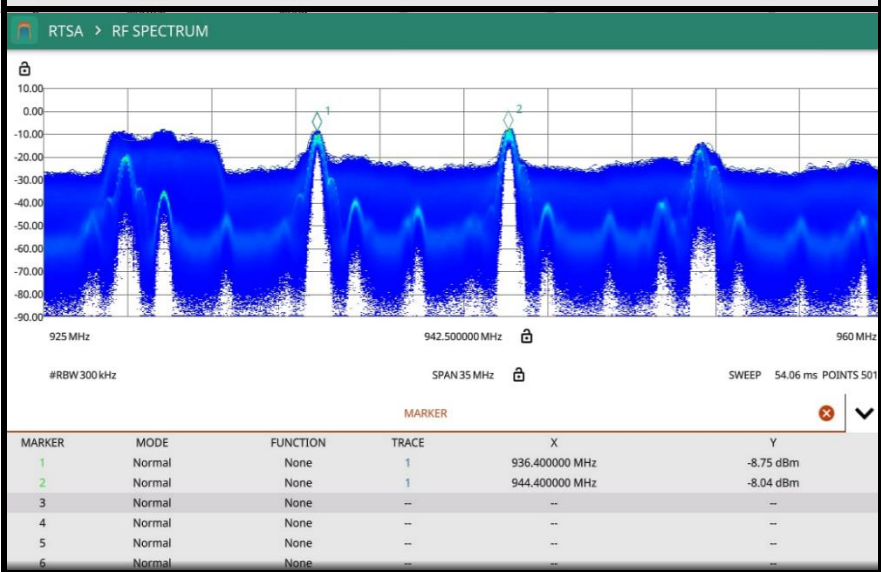


Figure.2. 900 MHz radio frequency measurement results from Fake BTS

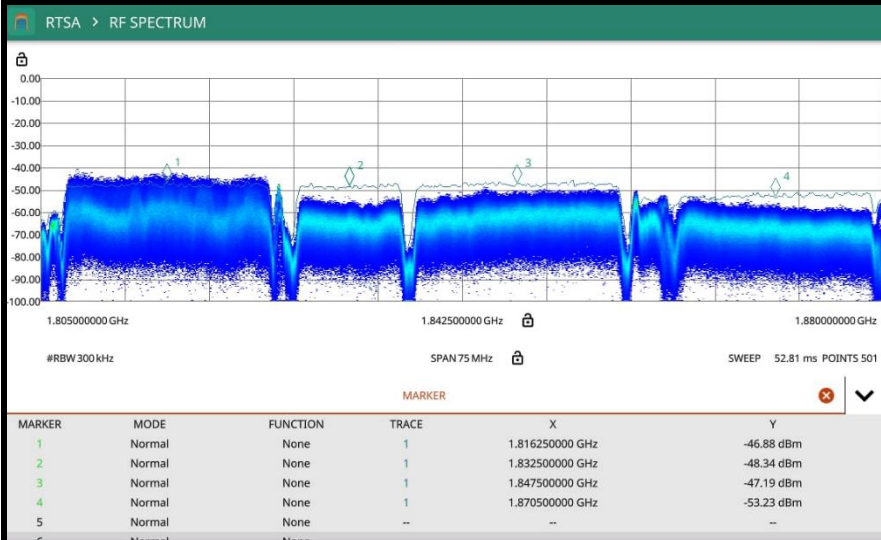


Figure.3. Measured results of 1800 MHz radio frequency of the Official BTS



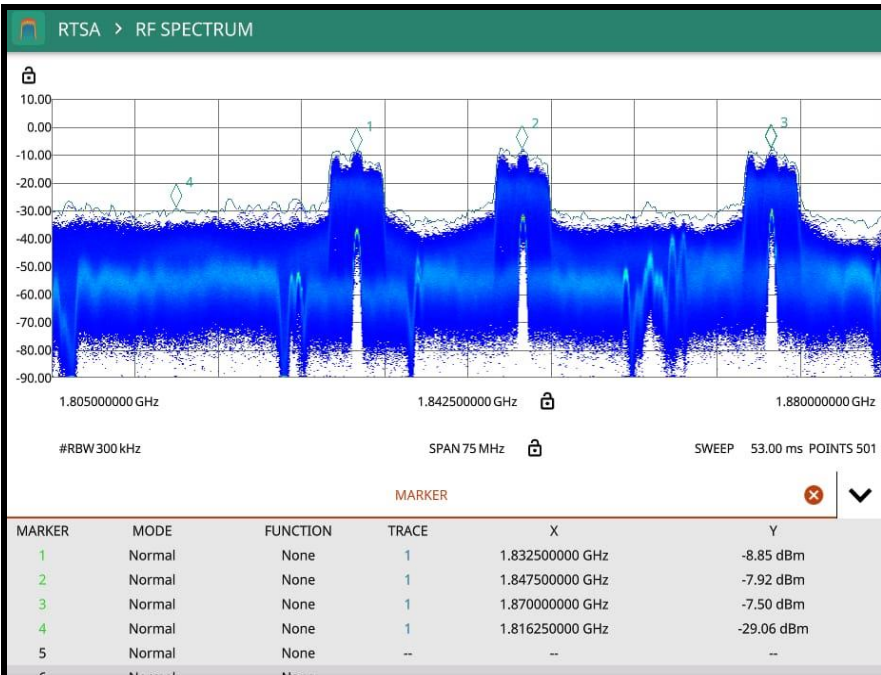


Figure.4. 1800 MHz radio frequency measurement results from Fake BTS

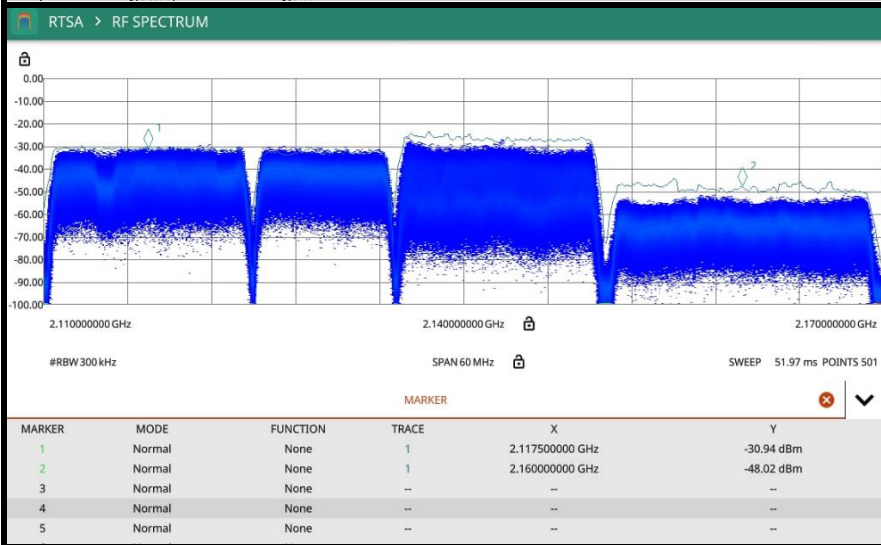


Figure.5. 2100 MHz radio frequency measurement results from Fake BTS

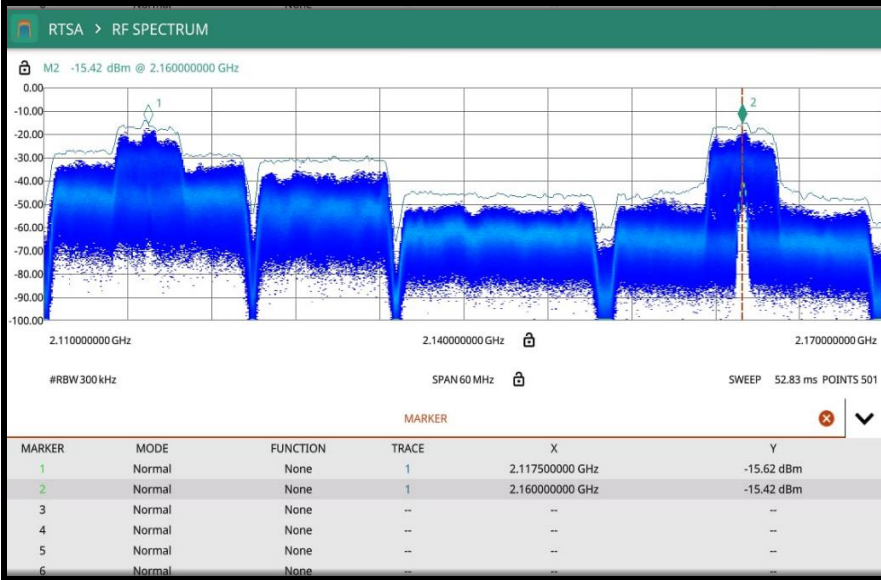


Figure.6. 2100 MHz radio frequency measurement results from Fake BTS

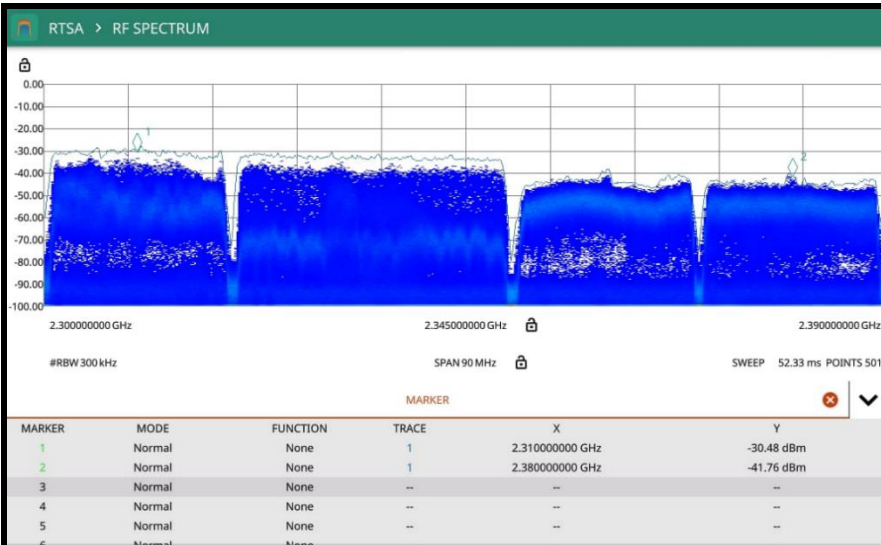


Figure.7. 2300 MHz radio frequency measurement results from Fake BTS

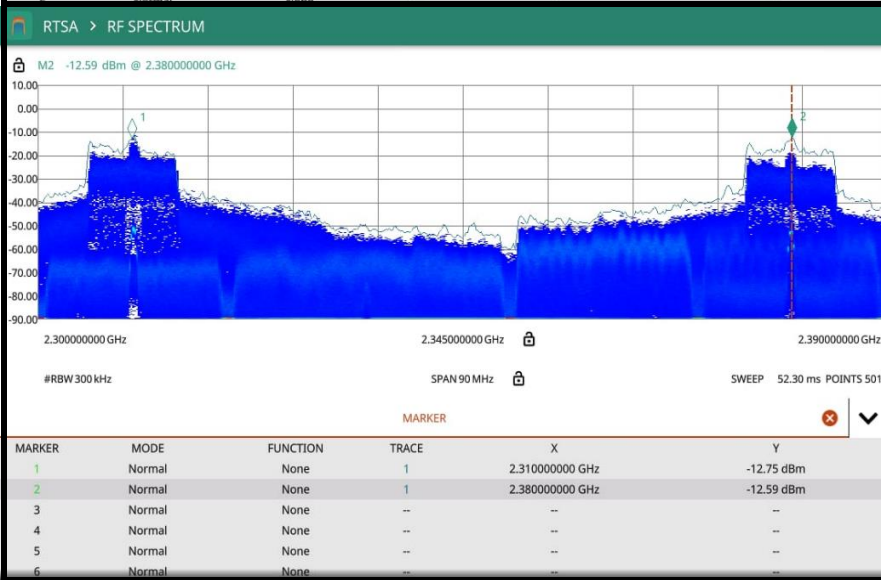


Figure.8. 2300 MHz radio frequency measurement results from Fake BTS





Figure.9. fake BTS indication of G-Nettrack application

Table 1. Comparative Analysis of Legitimate BTS and Rogue BTS Signal Attributes

Technical Parameter	Legitimate BTS	Rogue BTS
Frequency (MHz)	900 / 1800 / 2100 / 2300	Same as legitimate BTS (spoofed)
Signal Strength (RSRP)	-80 to -95 dBm	-60 to -70 dBm (stronger)
Signal Stability	Stable	Fluctuating / unstable
Network Technology	4G / 5G	2G (forced downgrade)
Cell ID Changes	Relatively stable	Frequent changes in a short time
Network Status	Connected, no errors	Emergency call only, frequent call drops
LAC/MNC/MCC Identification	Registered and valid	Does not match operator database
Signal Quality (RSRQ)	-8 to -11 dB	0 or unreadable

Source: Field Measurement Data (2025)

5. CONCLUSION

This investigation substantiates the existence and strategic utilization of

unauthorized base stations (counterfeit BTS) within the densely populated urban environment of Jakarta. Employing field

measurements facilitated by spectrum analyzers and the G-NetTrack application, the research uncovered signals exhibiting anomalous characteristics—such as excessive yet unstable strength, abrupt alterations in cell identity, and involuntary regressions to 2G networks—which are symptomatic of illicit transmission sources. These results address the fundamental research inquiry concerning the technical attributes and spatial distributions of rogue BTS operations. The study not only catalogs the empirical presence of such threats in Jakarta but also elucidates how these entities exploit systemic vulnerabilities in mobile network authentication protocols. The findings bolster the objective of furnishing empirical data that enhances the understanding, detection, and mitigation of counterfeit BTS threats within Indonesia's urban communication infrastructure.

Building upon these discoveries, it is advisable that subsequent initiatives concentrate on the development of integrated early warning systems that amalgamate real-time frequency monitoring with anomaly detection algorithms. Telecommunications operators, regulatory authorities, and security agencies should engage in collaborative efforts to establish routine signal audits,

particularly within high-risk locales such as government precincts and public congregating spaces. Furthermore, the revision of telecommunications regulations to encompass technical protocols for the identification and response to rogue BTS will be crucial. Lastly, enhancing public awareness and conducting internal training for field engineers on the recognition and reporting of suspicious signal activity can further fortify the national cellular network defense infrastructure.

## ACKNOWLEDGEMENTS

We extend our heartfelt gratitude to all individuals who provided their unwavering support during the duration of this research endeavor. Our profound appreciation is directed towards the technical and field teams, whose indispensable efforts were crucial in the acquisition of signal data from various urban locales in Jakarta. Furthermore, we express our sincere thanks to duty executor head of radio frequency spectrum monitoring center class I Jakarta, Head of Monitoring and Controlling Team SFR dan APT Balai Monitor SFR Kelas I Jakarta, PFR Balai Monitor Kelas I Jakarta for granting access to the requisite tools and facilities that facilitated the execution of this study.

## REFERENCES

- [1] ITU, "Measuring digital development: Facts and figures," International Telecommunication Union, 2021.
- [2] Y. Zhou, A. Alshamrani, A. S. Uluagac, "Cellular network security: Threats, architecture, and new directions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 356–379, 2019.
- [3] V. Nguyen, X. Lin, and H. Li, "Understanding 5G security: Challenges and opportunities," *IEEE Network*, vol. 35, no. 2, pp. 88–95, 2021.
- [4] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proc. 23rd Annual Network and Distributed System Security Symposium (NDSS)*, 2015.
- [5] S. Hussain, O. Chowdhury, and A. Yip, "Privacy attacks on 4G cellular paging," in *Proc. ACM CCS*, 2021, pp. 1137–1150.
- [6] D. Arik and M. Poznanski, "Cyber threats to mobile networks," *Journal of Cybersecurity*, vol. 4, no. 3, pp. 27–35, 2016.
- [7] A. Abdalla and M. Tariq, "False base station detection using signal fingerprinting," *IEEE Access*, vol. 11, pp. 25438–25450, 2023.
- [8] L. Rupperecht, A. Dabrowski, T. Holz, E. Weippl, and P. Teufl, "Breaking LTE on layer two," in *Proc. IEEE Symposium on Security and Privacy (S&P)*, 2018, pp. 1121–1136.
- [9] R. Karim, Z. Fatima, and M. Shah, "Mobile network vulnerabilities: An overview," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1893–1916, 2022.
- [10] J. Park, H. Lee, and Y. Kim, "Exploring IMSI catcher detection methods," in *Proc. ACM WiSec*, 2020, pp. 1–11.
- [11] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI catch me if you can: IMSI-catcher-catchers," in *Proc. Annual Computer Security Applications Conference (ACSAC)*, 2014.
- [12] M. Marzouki, R. Boutaba, and I. Ahmad, "Security risks of fake base stations in 5G networks," *IEEE Network*, vol. 35, no. 3, pp. 52–58, 2021.

- [13] S. Han, Z. Wu, and X. Wang, "Threat intelligence for 5G: Detection of rogue base stations," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1189–1202, 2022.
- [14] M. Lanz, D. Schmidt, and K. Biedermann, "Analyzing the risks of rogue LTE base stations," in *Proc. IEEE CNS*, 2020, pp. 1–9.
- [15] H. Kim, J. Lee, and C. Park, "Mobile network surveillance and IMSI catcher detection: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2598–2631, 2022.
- [16] Pemerintah Republik Indonesia, *Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi*, Jakarta, 1999.
- [17] Pemerintah Republik Indonesia, *Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi*, Jakarta, 2000.
- [18] Kementerian Kominfo RI, *Peraturan Menteri Kominfo Nomor 13 Tahun 2019 tentang Penyelenggaraan Telekomunikasi*, Jakarta, 2019.
- [19] Pemerintah Republik Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Jakarta, 2022.
- [20] A. Shaik et al., "A comparative study of LTE IMSI catchers," in *Proc. Black Hat Europe*, 2015.
- [21] 3GPP, "Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification," 3GPP TS 36.331, 2022.
- [22] H. Patel and A. Qureshi, "Detection techniques for GSM/UMTS/LTE rogue base stations," *International Journal of Security and Networks*, vol. 15, no. 2, pp. 75–84, 2021.
- [23] B. Lee and M. Choi, "Real-time rogue BTS detection using machine learning," in *Proc. IEEE ICICS*, 2023, pp. 19–24.
- [24] P. B. Rysavy, "Security in Mobile Wireless Networks," *IEEE Wireless Communications*, vol. 26, no. 2, pp. 10–17, 2019. (Topik: Keamanan jaringan seluler dan risiko BTS palsu)
- [25] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 84–90, 2019.
- [26] R. Borgaonkar, K. Redon, and J.-P. Seifert, "Security analysis of cellular protocols: A signaling perspective," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 2, pp. 61–69, 2014.
- [27] A. A. Adepu and A. Mathur, "Anomaly detection in a digital substation using power profiles," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4501–4511, 2018.
- [28] N. Asokan et al., "Mobile network security: Issues, challenges, and research directions," *IEEE Security & Privacy*, vol. 20, no. 1, pp. 12–21, 2022.
- [29] P. Zhang, J. Lin, and C. Shen, "Blockchain-based secure data sharing for Internet of Things in smart cities," *IEEE Access*, vol. 7, pp. 56356–56368, 2019.
- [30] M. K. Ismail and N. A. Ahmad, "Review of machine learning applications in detecting rogue base stations," *Journal of Information Security and Applications*, vol. 59, p. 102873, 2021.
- [31] A. H. Lashkari et al., "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Computers & Security*, vol. 92, p. 101762, 2020.
- [32] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in LTE-Advanced networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 1923–1940, 2015.
- [33] H. Wang, X. Wang, and J. Liu, "Privacy-aware efficient fine-grained access control for cloud storage with policy updating," *IEEE Transactions on Cloud Computing*, vol. 7, no. 2, pp. 476–489, 2019.
- [34] Y. Liu, D. Yang, and X. Shen, "Enhancing the security of cloud-assisted Internet of Things systems via blockchain," *IEEE Network*, vol. 33, no. 5, pp. 54–60, 2019.
- [35] T. D. Hoang and H. Nguyen, "Rogue BTS detection via signal pattern anomaly recognition using deep learning," in *Proc. IEEE International Conference on Communications (ICC)*, 2023, pp. 1–6.