City Research Online

City St George's, University of London

Citation: Saedi, M., Moore, A., Jafaar, F., Rahman, A. & Biswas, S. (2026). Zero Trust Rule-Based Protocol for Secure 5G Handover Against Rogue Base Stations. IEEE Open Journal of the Communications Society, 7, pp. 5092-5106. doi: 10.1109/ojcoms.2026.3691214

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/37405/

Link to published version: https://doi.org/10.1109/ojcoms.2026.3691214

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

OJ Logo

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version 11 January, 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.011100

Zero Trust Rule-Based Protocol for Secure 5G Handover Against Rogue Base Stations

MOHAMMAD SAEDI[1], *Member, IEEE*, ADRIAN MOORE[2], FEHMI JAFAAR[3], *Member, IEEE*, MD ARAFATUR RAHMAN[4], *Senior Member, IEEE*, and SUJIT BISWAS [1], *Senior Member, IEEE*

[1]Department of Computer Science, City St George's, University of London, EC1V 0HB, London, U.K.
[2]School of Computing, Ulster University, BT15 1ED, Belfast, , U.K.
[3]Département d'informatique et mathématique, Université du Québec à Chicoutimi, Chicoutimi, QC G7H 2B1, Canada
[4]School of Engineering, Computing & School of Mathematics and Computer Science, University of Wolverhampton, WV1 1LY Wolverhampton, U.K.

Corresponding author: Mohammad Saedi (e-mail: mohammad.saedi@citystgeorges.ac.uk).

This work was supported by the Pump Priming Research Scheme at City, St George's, University of London, and by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant Program.

ABSTRACT The 5G network has improved Rogue Base Stations (RBS) detection by concealing subscription permanent identifiers, and other security mechanisms passed down from legacy network generations to 5G. However, even with these enhancements, 5G is still vulnerable to RBS threats. A malicious actor can broadcast a signal of sufficient power to impersonate a legitimate base station, thereby deceiving the user devices into connecting to the rogue and potentially compromising confidential info. This work designs and implements a novel zero-trust-based network-side detection system for RBS threats that operates through the filtering of Measurement Reports (MRs). The proposed model introduces a probation period, during which candidate base stations are excluded from handover decisions while their legitimacy is continuously validated. We propose a trust analysis component to implement the RBS detector, initially using rule-based approach. The proposed model is augmented with an extended handover protocol that systematically excludes suspected RBS. We also show that the model employs a realistic dataset of radio signal measurements collected from a vehicle traversing various road segments. This scenario provides a practical use case demonstrating the framework's potential to enhance mobile network protection. The suggested model's performance results show that in the case of a big dataset comprising 1000 base stations and 180 rogue agents, the accuracy is 0.98, incorrectly classifying fourteen RBS as legitimate, and sets a new standard procedure for RBS identification.

INDEX TERMS 5G networks, zero trust network protocol, rogue base station detection systems, 5G network handover protocol, measurement reports, Radio access network

I. Introduction

In 5G networks, a User Equipment (UE) must first perform a cell search [1] to find available cells, achieve synchronization, and identify the serving cell before initiating communication. The UE can then perform a random access procedure after the initial cell search and gathering of system information to access the cell. The UEs start performing cell searches once they are activated; choosing a suitable cell involves finding and selecting it for connecting to the network. Accordingly, the UE performs signal strength measurements on neighboring gNodeBs and selects the strongest one. In a 5G mobile network, a UE is transferred from a serving Base Station (BS) to a target BS via handover procedures. The handover procedure is essential to ensure that mobile devices and UEs can travel across cells while maintaining high-quality network connectivity. The UE can be an Internet of Things (IoT) device equipped with mobile network capabilities, enabling it (or its subscriber) to connect

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

TABLE 1. List of Abbreviations Used in

Abbreviation	Definition
3GPP	Third Generation Partnership Project
5G	Fifth Generation Mobile Network
6G	Sixth Generation Mobile Network
3GPP	3rd Generation Partnership Project
GSM	Global System for Mobile
gNB	gNodeB (5G Base Station)
GUTI	Globally Unique Temporary Identity
IIoT	Industrial Internet of Things
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
LBS	Legitimate Base Station
ML	Machine Learning
MR	Measurement Report
NIST	National Institute of Standards and Technology
NR	New Radio
O-RAN	Open Radio Access Network
PCI	Physical Cell Identifier
RAN	Radio Access Network
RBS	Rogue Base Station
RoCH	Rate of Change (of Received Signal Strength)
RRC	Radio Resource Control
RSS	Received Signal Strength
SUPI	Subscription Permanent Identifier
UE	User Equipment
V2X	Vehicular to Everything

to a service provider to use a communications service [2]. A gNodeB oversees UE roaming between networks and also handles radio traffic, handover, and wireless security. In 5G networks, communication between the UE and the gNodeB is managed by the Radio Resource Control (RRC) protocol, which operates at Network Layer [3].

Since the beginning of GSM networks, Rogue Base Station (RBS) threats have continued to evolve and persist. Some improvement in RBS identification has been achieved following 5G and beyond networks. These include concealment of the Subscription Permanent Identifier (SUPI), replacement of 5G Globally Unique Temporary Identifier (5G-GUTI), and a generalized information-based detection approach, while other security mechanisms carried over to 5G network protection from legacy network generations include mutual authentication between the network and UE, secure cryptographic algorithm negotiations, and integrity-protected signaling [4]. Despite these developments, 5G is still vulnerable to RBS attacks [5]. We address this issue through zero trust principles [6], requiring continuous verification of BS legitimacy to avoid rogue exploitation. The RBS treatment efficacy varies greatly throughout cellular network generations, but they remain critical because of the multiple interconnections between a wide variety of current and legacy networks [7].

The process primarily relies on MR filtering, where detection occurs when the gNodeB receives the MRs gathered by UEs. The detector spots suspected RBS and removes them from the MR prior to its transmission to the currently connected gNodeB. This ensures that the suspected RBS are not included in the version of the MR utilized for the handover decision. Following the established handover protocol [8], [9], the UE communicates the MR to the connected gNodeB, which is responsible for recognizing the necessity for a handover and initiating the protocol. Since the gNodeB acts on the information provided by the UE, it makes sense that the detector should eliminate any Received Signal Strength (RSS) data coming from suspected RBS [10]. If the RBS data is not in the MR, it can never be the target of a handover event.

The main contributions are as follows:

- **Novel zero trust-based RBS detection system:** Introduces a network-side architecture at the gNodeB that filters MRs using a probation period and signal Rate of Change (RoCH) analysis to identify and block rogue agents proactively, achieving high accuracy while minimizing computational overhead in real-time mobile scenarios (Section IV).
- **Extended handover protocol with quarantined states:** Extends the standard 3GPP handover process by incorporating a ”Blocked” state for suspected RBSs, enabling continuous verification, proactive rejection, and reducing vulnerability windows during the migration of UE, while taking into account velocity-dependent thresholds and urban interference effects (Section E).
- **Integration into gNodeB architecture:** Integrates the RBS detection system within the 5G radio access layer for seamless network-side deployment, which ensures compliance with 3GPP standards, scalability across diverse environments like V2X platooning, and robustness against coordinated RBS attacks without requiring UE modifications (Sections III and IV).
- **Rule-based trust analysis algorithm:** Proposes a sliding window mechanism for continuous RoCH monitoring during the probation period, with detailed implementation for classifying BS legitimacy, including edge cases such as unreliable signals or low RoCH variations, and discusses adaptability to variables such as base station signal power and UE mobility (Sections V).
- **Comprehensive performance evaluation and implications:** Analyzes simulated datasets with different BS/RBS densities (e.g., 1000 BSs and 180 RBSs), demonstrating 98% accuracy with low false negatives (FN=14), alongside nuanced discussions on high-density multipath vs isolated signals deployments, real-world limitations like threshold variability, and future extensions to Machine Learning (ML) to improve real-time classification (Section VI).

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

The remainder of this paper is structured as follows. Section II reviews RBS detection methods related work and highlights their limitations. In Section III we present the 5G BS handover process, and then in Section IV, we propose the RBS detection system, introduce the RoCH feature for signal analysis (Section A), analyze MR data (Section B), and define probation period for initial BS monitoring (Section C), and then, implement handover process in detail (Section D), taking into account real-world variables such as UE mobility and environmental noise. Then, in Section V, we design the BS trust analysis component, which details the trust analysis algorithm to implement RBS detection, covering the sliding window mechanism (Section A), the core algorithm (Section D), and Section E, then offers an extended handover protocol to reject suspected rogues, including edge cases like intermittent signals. Section VI provides a performance analysis of the proposed method on simulated datasets, identifying limitations such as threshold variability and discussing implications for urban vs. rural deployments. Finally, Section VIII sums up key findings and provides an overview of future work, such as how adaptive thresholds can be incorporated with ML.

II. Related Work

The detection of RBS attacks in 5G networks has been extensively studied, with various methods proposed to enhance network security. These methods can be broadly categorized into UE-side, cloud-based, and network-based approaches [2], [11].

The most recent RBS detection systems incorporate a data collection feature within the UE which be able to analyze the data collected from the IoT devices, which is known as UE-side detection [8], [12], [13], or it sends the gathered data to a central server, known as cloud-side detection [9], [11], or sends it to the network, for example, the radio access layer, for examination, which is categorised as network-based detection systems [14]. The first group is more likely to produce FP, because a UE is unable to comprehend the comprehensive status of the network view at any given time. In addition, the UE-side detection techniques frequently require changes such as software updates on the device or root access, both of which may be difficult and even impossible for certain users to accomplish. Cloud-based techniques collect the MRs from UEs to a central 5G core server for processing (e.g., FBS-Radar) [11]; however, they keep UE-side efficiency limitations while adding scalability and privacy concerns.

Network-based detection systems are projected to perform better in terms of analysis since, in contrast to UEs, mobile networks are aware of the system's status on a global scale. However, to collect data from different network locations or protocols, there must already be an established monitoring infrastructure in place. Murat [7] exemplifies multi-RAT RBS identification using operational data. Our proposed method differs by focusing entirely on the network side, specifically the gNodeB. Network-based solutions are less explored but offer significant potential for improving detection accuracy and reducing FP. Singh et al. [15] explored signal monitoring at gNodeBs, laying the groundwork for our approach. This research focuses on network-based detection since it is more appropriate for 5G and cellular networks [16]. Several techniques have been proposed to detect RBSs, primarily relying on physical layer characteristics such as signal strength, timing advance, and propagation models [17]. However, these techniques often suffer from high FP rates and may fail to detect sophisticated RBSs that can mimic Legitimate Base Station (LBS) characteristics. Another category of detection approaches involves monitoring network traffic and control plane messages for anomalies [18]. While effective in some cases, these methods can be computationally expensive and may require modifications to existing network infrastructure.

Secure handover mechanisms are crucial for ensuring seamless mobility and maintaining communication integrity during handovers in cellular networks. Existing protocols, such as those specified by the IEEE 802.21 and 3GPP standards, employ techniques like encryption, authentication, and key management to secure the handover process [19], [20], [21]. However, these protocols often introduce significant overhead and complexity, which can be challenging to implement on resource-constrained mobile devices and networks. Additionally, context-aware and adaptive handover decision mechanisms have been proposed to improve handover performance, but they typically do not consider security aspects or RBS threats.

Moreover, several studies have investigated the use of dedicated monitoring nodes or crowdsourcing approaches to detect RBS [7], [11]. Monitoring nodes are specialised devices deployed in the network to analyze signals and traffic patterns for potential anomalies. While effective in controlled environments, this approach may not be scalable or cost-effective for large-scale deployments. Crowdsourcing techniques, on the other hand, leverage user devices to collect and report data on suspected RBS. However, these techniques often face challenges related to incentivising user participation, ensuring data privacy, and dealing with potentially unreliable or malicious reports. Furthermore, most existing RBS detection techniques focus on identifying individual RBS but may not be effective in detecting coordinated attacks involving multiple rogue base stations working in tandem.

A. Comparison and Gap Analysis

While existing methods provide valuable insights into RBS detection, they often suffer from high FPs, scalability issues, or latency concerns. UE-side solutions are limited by the computational capacity and environmental factors affecting signal quality. Cloud-based approaches, although powerful, introduce latency and privacy issues.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

TABLE 2. RBS detection approaches: A Qualitative comparison

Approach	Expected Accuracy	Computational Overhead	Latency	Deployment Complexity	Main Characteristics
UE-side detection	Moderate	Low to moderate (device-side)	Low	High, due to device modification or software requirements	Local visibility, easy to personalize, but limited global network awareness and higher false-alarm risk
Cloud-based detection	Moderate to high	High	Moderate to high	High, due to centralized data collection and processing	Stronger centralized analysis, but increased transport overhead, privacy concerns, and slower reaction
ML-based detection	Potentially high	High	Moderate	High, due to training, tuning, and model maintenance	Better adaptability in complex scenarios, but requires larger datasets and may be harder to integrate in real time
Our work	High in structured scenarios	Low	Low	Moderate	Lightweight, directly integrated with handover control, no UE modification required, but less adaptive than ML in complex edge cases

Hybrid methods, although promising, require complex coordination between UE and network components, which may not be feasible in real-time scenarios. Many of these methods demand inherent trust in BS signals, which is a gap our zero trust-based solution addresses by requiring continuous verification [22]. Our network-based solution addresses these gaps by implementing detection entirely at the gNodeB, introducing a probation period for new base stations, and employing a trust analysis mechanism to accurately and efficiently detect rogue base stations [18], [23]. This approach not only reduces the FP but also ensures real-time detection without overburdening the UE or compromising data privacy.

B. Qualitative Comparison with Alternative Detection Approaches

Table 2 provides a qualitative comparison between the proposed method and representative UE-side, cloud-based, and machine-learning-based approaches. The comparison considers detection accuracy, computational overhead, latency, deployment complexity, and compatibility with 3GPP handover procedures. As shown in the table, our work achieves a favorable tradeoff between detection capability, processing overhead, and deployment practicality, especially for real-time handover protection.

III. 5G Base Station Handover

Figure 1 illustrates the 5G inter-gNodeB handover process. The UE in RRC_CONNECTED mode receives measurement configuration data provided by the network, including the radio frequency channel numbers and specific trigger criteria. When these criteria are met, for example, when a signal power level of the UE from the source eNodeB falls below a predefined threshold, the UE sends an MR to the serving gNodeB. This MR contains the Physical Cell Identifiers (PCI) and the corresponding power measurements of the nearby cells visible to UE on the configured radio frequency channel(s) [4], [9]. When a handover is needed,

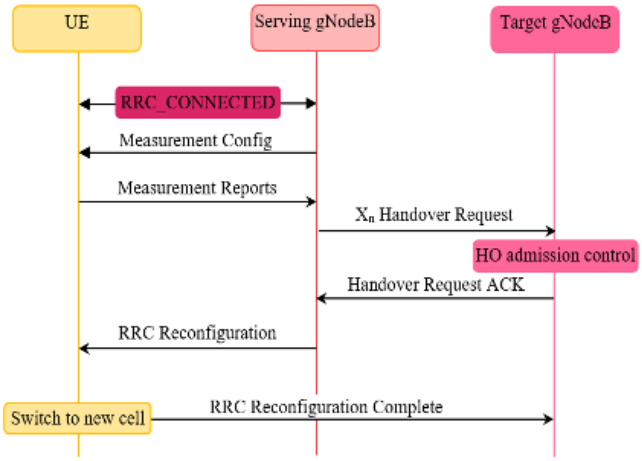

FIGURE 1. 5G inter gNodeB handover.

the serving gNodeB initiates the process through the Xn interface by sending an Xn Handover Request message to the target gNodeB, preparing for a handover. The target gNodeB makes the handover admission decision and prepares radio resources for the user equipment. In response, it sends a handover request acknowledgement to show that it is ready to accept the UE. Following that, the serving gNodeB sends the Handover Request ACK message to the UE, including the beam-specific information, cell ID, and access information. Then, the serving gNodeB sends a handover command to the UE along with an RRC connection reconfiguration message that includes destination gNodeB information, such as PCI, radio frequency channel, etc. The UE then moves into the RRC_connected state with the target gNodeB and sends the RRC Reconfiguration Complete message.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

A. Handover Process

According to the 3GPP, the handover process identifies a BS with an RSS that exceeds that of the currently connected BS by at least the threshold level. Following the basis of handover in the 3GPP [4], the handover state machine is depicted in Figure 2, as detailed in section III. The current position with no rogue detection component includes two states and one pseudo-state. The ”Outside” pseudo-state represents a BS that does not appear in the MR, while the other two states indicate that a BS that appears in the MR is either a “Connected” or a ”Candidate”.

A new base station from the “Outside” state is discovered and integrated into the state machine. When a BS appears in the MR, it immediately qualifies as a ”candidate” for handover. The currently active BS is referred to as the “Connected” BS, and at any given time, there can be only one BS in this connected state for a UE. When the received signal of the new BS exceeds that of the connected BS by the threshold level, a handover will be initiated. If the currently connected BS drops out of the MR, it will be swiftly replaced by the strongest available candidate. The ”Drop Out” arc from both Candidate and Connected to the outside of the state machine clearly marks when a BS has exited the MR.

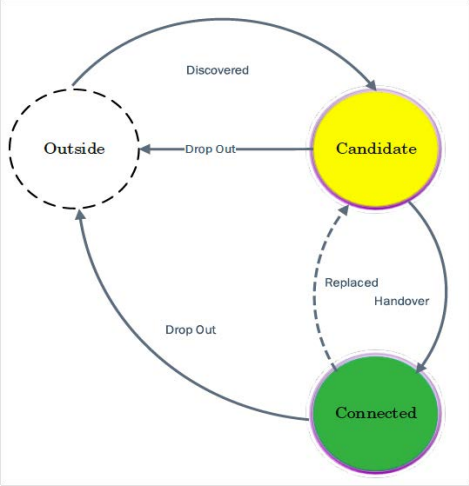

FIGURE 2. **The legitimate base station handover state machine.**

One of the key features used by the BS Analysis system to identify any fingerprint associated with the RBS is Rate of Change (RoCH), which is detailed in section A. Analyzing the RSS value ranges shows that the MR’s highest signal levels are around -70 and -75, while the lowest is around -90 and -95. These values are impacted by the distance between the BS and the road, as well as the BS transmission’s power. The graph in Figure 3 depicts an attack scenario in which RBS values grow and fall more quickly than LBS values. As a result, RBS has a much higher average RoCH rate than LBS during the early increase phase. Because the RoCH is dependent on the vehicle’s speed, the system must learn and modify the threshold accordingly.

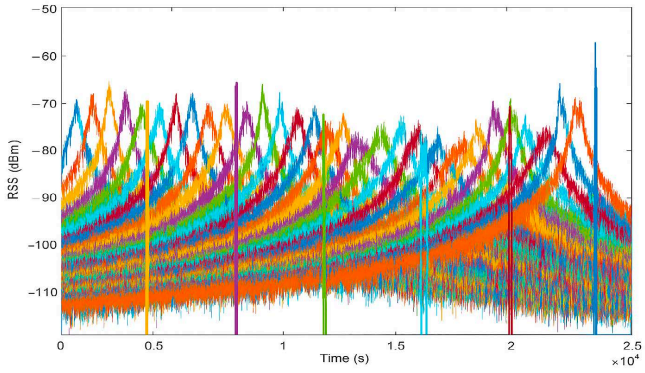

FIGURE 3. **Attack scenario.**

The Figure 4 shows the handover to RBS in the scenario. The periods when the platoon leader is connected to a legitimate BS are represented by a blue signal, and a red signal highlights connection to an RBS.

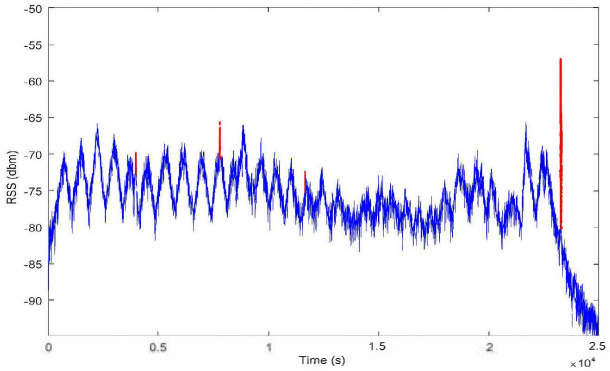

FIGURE 4. **Handover to rogue base station.**

IV. Proposed RBS Detection System

This section proposes our RBS-detection system to identify rogue agents in 5G networks, which is located at the gNodeB and blocks suspected RBS from the MR before applying the handover process. Figure 5 illustrates the architecture, which includes a BS probation period, a BS trust analysis, and an extended handover protocol. To prevent handover to any BS that has been in the MR for fewer than 10 continuous timestamps, the candidate BS is monitored during the probationary period. This is an estimated duration of the probationary period to be examined and offers a window of opportunity for verifying a BS’s status before its consideration for handover. The approach used to figure out whether a BS is legitimate or rogue is called the BS trust analysis. The design develops a classification based on the RSS values and also the RoCH after processing sequential MR inputs from a single BS. To implement the RBS detection system, the trust analysis component is suggested; it will be further discussed in Section V.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

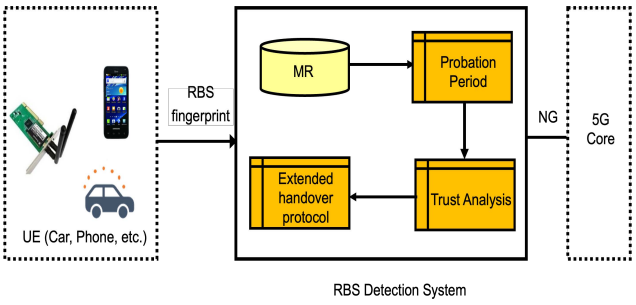

FIGURE 5. Proposed RBS Detection System.

The final component of the RBS detection system is a proposed handover protocol, extending the existing one to introduce a new "blocked" state in order to manage the BS status for a potential handover after having the outcome of the BS trust analysis component. For UEs to be able to roam freely between cells while maintaining high-quality communication services, handover control is crucial. The UE motion between cells is controlled by the gNodeB. In the 5G RAN, the MR produced by UEs is typically the foundation for the handover decision [24].

The primary method employed by the proposed system for identifying rogue base stations is based on the RoCH analysis of the received signal values during the probation period. The probation period component in Figure 5 is an important component of the RBS detection system, during which a newly discovered candidate base station is disqualified from consideration for handover. Instead, the RoCH of the RSS values reported by the UE for this candidate base station is closely monitored over the initial set of MR entries. A sharply increasing RoCH during this period is identified as a characteristic fingerprint of a potential rogue base station, as it tends to transmit higher-than-normal signal strength to lure nearby UEs.

The core of the RBS detection mechanism lies in the BS trust analysis component, which implements the RoCH-based analysis using a sliding window approach. For each candidate base station in the MR, a sliding window of the most recent signal RoCH or delta values (i.e., the differences between consecutive RSS values) is maintained. If the sliding window is full and does not contain any values exceeding a predetermined threshold, the candidate base station is classified as legitimate. However, if the sliding window exhibits a substantial jump in RSS, indicating a rapid increase in signal strength, the candidate base station is identified as a rogue base station and marked as "Blocked" in the proposed extended handover protocol.

When a new base station is detected in the MR received from the UE, the system does not immediately consider it a candidate for handover. Instead, the newly discovered base station enters a "probation period" during which its legitimacy is assessed. The window size of the probation period is set to $N = 10$ timestamps, which is used as a baseline configuration for the probation period in the proposed approach. The implications of this choice in terms of mobility and latency are analyzed in V.B and V.C . During this period, the new base station is assigned a "Blocked" state and is prevented from being involved in any handover decision.

The probation period serves as a crucial window of opportunity for the system to analyze the behaviour of the newly discovered base station and determine whether it exhibits characteristics of a rogue base station or not. Specifically, the BS trust analysis component monitors the RoCH of the RSS values reported for this base station during the probation period. A rapid increase in the RoCH, indicative of an abnormally high signal strength transmission, would trigger the classification of the base station as a rogue. Only after successfully passing the trust analysis and completing the probation period is the base station permitted to transition to the "Candidate" state, making it eligible for potential handover.

The handover process discussed in subsection A is the mechanism through which the UE is now connected to a serving base station (gNodeB), and the serving BS will commence a handover to another BS in the MR if its signal level is higher than the serving BS's by the threshold value. This handover can happen once a new BS with a sufficient RSS is identified, according to the current 3GPP standard. However, the initial high RoCH between subsequent MR entries is a potential identifier of the RBS. Following the introduction of a probationary period during which newly discovered BSs are disqualified from handover, the RoCH within that initial set of MR entries is analysed.

A. Signal Rate of Change Feature

An RBS typically generates a higher signal power to attract the surrounding UEs. A sharp increase or sharp fall in signal level [18], [25] succinctly captures the identity of an RBS and provides a distinctive fingerprint for detection.

The trust analysis component of the RBS Detector implements a new RoCH feature that is monitored for all LBS and RBS detected by a UE. The RSS from the currently connected BS, e.g., BS1, gradually decreases as the UE moves away, while the RSS from a candidate BS, e.g., BS2, increases accordingly. During the probation period, the initial monitoring window from the BS's first detection until 10 consecutive MR values are accumulated, the RoCH of BS2 would reflect a steady and predictable slope influenced by the UE's speed and path loss. This period begins at the timestamp when the candidate first appears in the MR and continues until sufficient data confirms stability, aligning with handover triggers like the point where BS2 exceeds BS1 by a predefined threshold (e.g., 5 dB) [26]. Section 6 will discuss a minimum probation period.

However, an RBS scenario features sharper dynamics: The rogue signal increases rapidly to dominate the MR, often

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

before handover, then drops as the UE exits its range. This continuous analysis enables proactive rogue exclusion independent of handover. Scenarios vary based on the LBS/RBS appearances in the MR concurrently, e.g., overlapping in urban density vs isolation in rural areas. To prevent hijacking, identified rogue agents must be prohibited from handover. From a complex perspective, RoCH thresholds vary with UE velocity (e.g., raised rates in high-speed platooning) [10], base station power, and ambient variables (e.g., urban multipath fading resembling spikes [27], [28]. This approach would enhance real-time reliability via low-overhead filtering over ML alternatives [29], potentially cutting FNs by 10-20% in mobility contexts per recent IIoT studies [18]. O-RAN integration for programmable monitoring and 6G AI for threshold adjustment [30] are related factors. Overall, this RoCH approach provides a robust, standards-compliant foundation for RBS mitigation, balancing simplicity and efficiency over 5G environments.

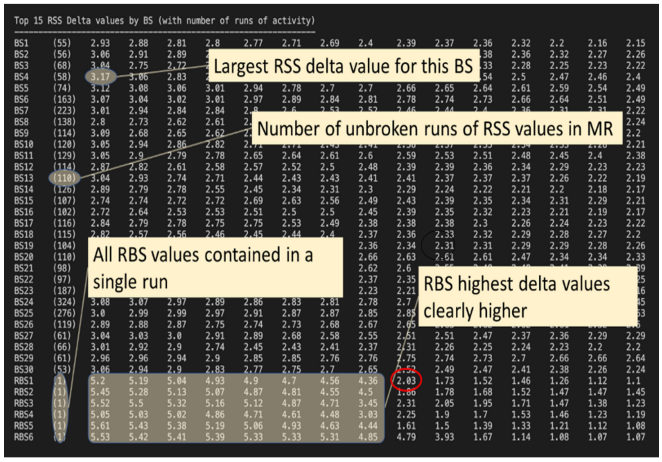

FIGURE 6. Rate of change description, the Top 15 received signal rate of change or RSS delta, for legitimate and rogue base stations.

B. Measurement Report Data Analysis

Our case study includes several scenarios on detecting RBS using a realistic dataset of radio information and RSS measurements that was generated by a vehicle simulation on a variety of road sections for identifying characteristics for developing a detection model. The numerical modelling set used in this research can replicate several BS and RBS throughout a large highway, as detailed in [31].

Figure 6 presents the 15 most significant differences in consecutive RSS values for each BS based on a simulation of 30 BSs and six RBSs, sorted by size. The largest change observed for BS1 between two consecutive timestamps is 2.93, while the second RoCH or delta for BS1 is 2.88. RoCH denotes the difference between successive signal entries in the MR. The first column represents the BS identifiers, including 30 LBS and 6 RBS. The second column shows, in parentheses, the number of consecutive appearance sequences of each BS in the MR. For example, BS13 appears in 110 such sequences. Most sequences are short as the signal rises and then falls, while sequences near peak signal strength tend to be longer and more stable. Examining the values shows that the largest delta for any legitimate BS is 3.17. All delta values exceeding this threshold are produced by the rogue agents in the final rows of the table, and the eight highest deltas from each RBS are significantly greater than those from legitimate BSs.

Beyond the top eight entries, the delta values of the RBSs become numerically indistinguishable from those generated by a legitimate BS. For example the highlighted RBS delta value of 2.03 (marked by a red circle in Figure 6) could readily be misinterpreted as originating from a valid BS. However, a complementary observation enables more reliable classification. As shown in the second column, RBS entries within each MR consistently appear in a single continuous run; once an RBS enters the MR, it persists until reaching its peak signal level and subsequently begins to decline. Therefore, the presence of a sustained sequence of high delta values in the MR is used as a strong indicator for RBS identification. In summary, deltas above 3.17 can indicate an RBS, which must be classified after a probation period in the MR before handover is considered.

C. Probation Period Component of RBS Decector

Table 3 displays a data frame of MR data spanning timestamps 3529-3565, making when and how a new candidate is evaluated for a handover.

The MR records six powerful signals at every timestamp, so an empty entry means the BS simply is not among the top six, rather than having no signal. e.g., at timestamp 3529, the MR contains RSS values from BS2 to BS7. BS8 first appears at timestamp 3530; however, it becomes consistent only from 3554 onwards. It is regarded as a handover candidate after remaining in the MR for a probation period.

The probation period is critical; once completed, a handover will be triggered if the RSS is sufficient, as shown in Table 3. For BS8, the red-boxed values mark its probation period, and the earliest time it might be regarded for handover. Therefore, these values are used for the initial BS/RBS classification of BS8.

Figure 7 visualizes the time series diagram generated from Table 3. BS8 appears intermittently early on but emerges in the MR consistently after timestamp 3554 (highlighted by the connected black diamonds on the right), qualifying it as a new candidate BS. The MR only contains six strongest signals per timestamp; the top-six list updates to BS3-BS8 after 3554, while it was BS2-BS7 before that point.

D. The BS Handover Implementation

Handover decisions in 5G networks are based on the MR produced by UEs [24]. A UE remains connected to its serving BS until another BS in the MR exceeds the current one by a defined threshold; at that point, handover occurs.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

TABLE 3. Newly discovered candidate base stations

Time	BS2	BS3	BS4	BS5	BS6	BS7	BS8
3529	-90.84	-89.38	-78.62	-79.71	-84.63	-92.90	
3530	-90.23	-89.90	-79.14	-78.56	-84.36		-93.01
3531	-90.25	-89.61	-81.42	-79.27	-84.25	-92.22	
3532	-90.24	-90.48	-82.55	-78.54	-84.47	-91.40	
3533	-90.35	-90.05	-82.66	-78.28	-84.63	-91.83	
3534	-91.14	-90.45	-82.71	-77.46	-84.83		-92.48
3535	-91.60	-90.70	-84.49	-75.54	-85.14		-92.58
3536	-92.54	-89.16	-85.05	-74.53	-85.80		-92.37
3537	-92.09	-88.98	-84.39	-74.14	-84.85	-92.41	
3538	-92.08	-88.94	-84.44	-74.27	-84.57	-92.45	
3539	-92.09	-89.06	-84.85	-74.24	-84.67	-91.47	
3540	-94.01	-87.62	-84.63	-74.24	-84.58	-91.42	
3541	-93.95	-87.97	-83.18	-73.90	-84.39	-90.10	
3542	-93.90	-87.02	-82.70	-75.04	-84.76	-90.29	
3543	-94.13	-88.11	-83.10	-75.20	-85.28	-89.70	
3544	-93.16	-87.95	-83.66	-75.66	-85.03	-88.70	
3545	-92.72	-88.24	-82.16	-75.52	-85.01	-88.39	
3546	-91.80	-88.16	-81.18	-75.22	-84.22	-88.21	
3547	-92.05	-87.90	-81.43	-75.23	-84.36	-88.76	
3548	-91.77	-87.91	-81.41	-76.03	-83.95	-89.17	
3549	-91.51	-87.88	-81.13	-76.11	-83.70	-89.06	
3550	-89.63	-88.12	-80.90	-76.15	-83.68	-89.88	
3551	-91.85	-88.37	-80.22	-75.74	-83.73	-89.56	
3552	-91.72	-88.33	-79.95	-74.68	-83.31	-90.05	
3553	-92.23	-87.98	-79.68	-74.30	-83.98	-90.25	
3554	-87.57	-78.98	-73.85	-84.61	-89.93	**-92.58**	
3555	-87.32	-79.00	-74.13	-84.28	-89.95	**-91.99**	
3556	-87.38	-79.23	-73.72	-84.25	-89.40	**-92.19**	
3557	-87.27	-80.10	-73.72	-84.14	-88.91	**-92.39**	
3558	-86.66	-80.15	-72.77	-84.58	-88.42	**-92.15**	
3559	-87.82	-80.27	-72.76	-84.45	-88.41	**-92.31**	
3560	-88.61	-80.36	-72.66	-84.54	-87.71	**-92.45**	
3561	-88.34	-80.96	-72.76	-84.49	-87.78	**-92.68**	
3562	-88.65	-81.04	-72.63	-84.32	-88.37	**-92.44**	
3563	-88.89	-81.06	-72.56	-83.94	-88.83	**-91.72**	
3564	-89.80	-80.99	-71.99	-83.60	-90.03	**-91.82**	
3565	-89.70	-82.32	-71.72	-83.95	-91.16	**-92.42**	

Table 4 shows this process in a snapshot form, presenting MR data from timestamps 1273 to 1284 to demonstrate that the serving BS can be handed over to the new strong gNodeB. According to the 3GPP, a candidate BS should meet the handover trigger threshold. In this example, the handover threshold [26] is assumed to be 5 dB. At t=1273, BS2 is stronger than BS1, but the difference reaches 5 dB at t=1279. With the falling signal of BS1 and BS2's rising, the gap exceeds the threshold at t=1279 (highlighted in yellow in Table 4), initiating the handover. The RSS values are expressed in dBm, where negative values are typical due to the logarithmic representation of received power relative to 1 mW. Algorithm 1 illustrates a simple implementation of how to model the handover procedure.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

Algorithm 1 Simulated Handover Procedure

Require: The candidate base stations vector **BS**
Ensure: Handover decision vector **Vector_HO**

Initialize variables: $timestamp$, $Serving_BS$, $WindowSize$, $Boundary$
Determine RSS indices for $Serving_BS$: $Serving_BS_R$ and $Serving_BS_C$
Construct the RSS vector $\mathbf{Vector_RSS}(\mathrm{RSS}(i), Boundary)$
$Serving_BS \leftarrow \max(\mathbf{Vector_RSS})$
$\mathbf{Vector_HO}(timestamp) \leftarrow Serving_BS$
$[Serving_BS_R, Serving_BS_C] \leftarrow find(\max(\mathbf{Vector_RSS}(timestamp, :)))$
while $t < TimeLimit - WindowSize$ **do**
  $Candidate_BS \leftarrow \max(\mathbf{Vector_RSS}(timestamp + 1, :))$
  $[Candidate_BS_R, Candidate_BS_C] \leftarrow find(\mathbf{Vector_RSS}(Candidate_BS))$
  if $Candidate_BS \geq \mathbf{Vector_RSS}(timestamp - 1, Serving_BS_C) + Threshold$ **then**
    $Serving_BS \leftarrow Candidate_BS$
    $Serving_BS_C \leftarrow Candidate_BS_C$
    $Serving_BS_R \leftarrow Candidate_BS_R$
  else
    $Serving_BS \leftarrow \mathbf{Vector_RSS}(Candidate_BS_R, Serving_BS_C)$
    $Serving_BS_R \leftarrow Candidate_BS_R$
  end if
  $\mathbf{Vector_HO}(timestamp + 1) \leftarrow Serving_BS$
  Update($timestamp$)
end while

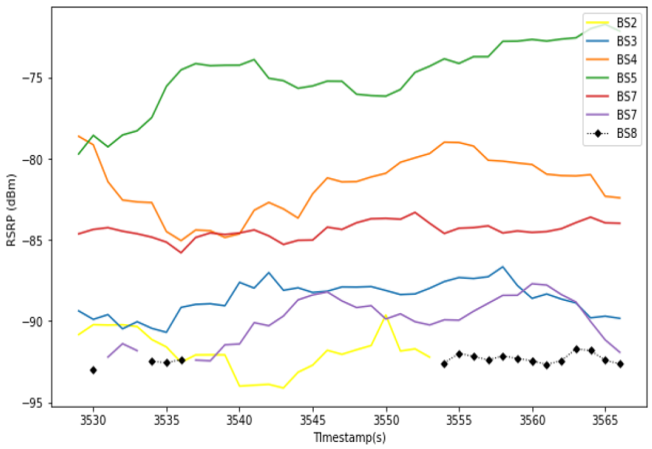

FIGURE 7. **Waveform diagram for the new candidate base station.**

TABLE 4. **Handover process demonstrated in a snapshot data**

Timestamp	BS1 (dBm)	BS2 (dBm)	BS2 - BS1 (dB)
1273	-78.20	-75.38	2.82
1274	-78.02	-75.32	2.70
1275	-77.88	-74.99	2.89
1276	-78.65	-74.61	4.04
1277	-78.64	-75.16	3.48
1278	-79.70	-74.81	4.89
1279	-79.56	-73.36	**6.20**
1280	-79.52	-72.93	6.59
1281	-79.63	-73.09	6.54
1282	-79.83	-72.80	7.03
1283	-80.22	-72.69	7.53
1284	-80.53	-72.46	8.07

V. Trust Analysis model for Rogue Base Stations Detection

This work presents a novel model for BS monitoring that explicitly accounts for the potential presence of rogue agents within the MR. Figure 8 demonstrates that the state machine is extended to incorporate a blocked state. Any BS that is appears in the MR and is identified as rogue is assigned to this state and therefore excluded from handover consideration. To facilitate analysis and classification of a new MR entry, the model introduce an initial trust assessment period during which the entry is excluded from being eligible for a handover. Base stations that successfully pass the analysis transition to the candidate state, and those that fail remain blocked.

The proposed model has three BS states:

- **Blocked**: A BS enters a blocked state when classified as rogue after failing the trust analysis. Newly discovered BS is also placed in the blocked state until they have appeared in the MR for the probation period.
- **Candidate**: A BS transition to this state after completing its probation period and passing the trust analysis. It can be eligible for handover if its RSS exceeds that of the currently connected BS by the specified threshold.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

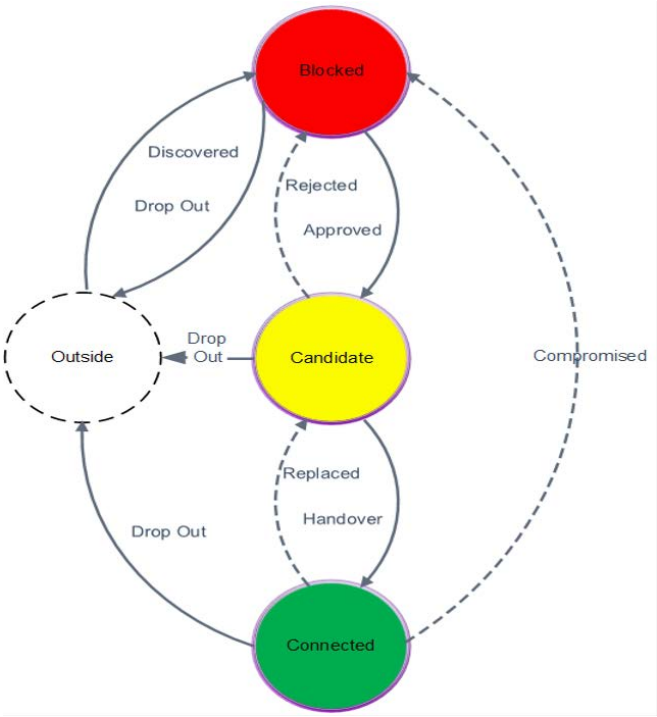

FIGURE 8. **The proposed rogue base station handover state machine**

- **Connected**: This state denotes the currently serving base station. Only one BS can occupy the connected state for any UE at any time.

Base stations transition between states based on the RSS values and continous trust analysis. A newly discovered BS moves from blocked to candidate after its probation period expires. It may then be promoted to connected if its RSS exceeds the serving BS's threshold. A displaced connected BS reverts to the candidate state if it remains in the MR. Trust analysis runs at every sample point for each BS in the MR; therefore, any trusted BS exhibiting rogue-like bahavior is promptly moved to blocked which may require a candidate to move to connected. Any BS exiting the MR from blocked, candidate or connected enters the Outside pseudo-state.

The Trust analysis model aims to eliminate the transitions from candidate and connected states to the blocked state, represented by the dotted arcs in Figure 8, by detecting all RBS during their initial probation period while they remain blocked.

which is used as a baseline configuration for the probation period in the proposed approach

A. Received Signal Sliding Window Mechanism

This section introduces the sliding-window technique and then proposes the zero BS trust analysis algorithm. A sliding window of the most recent RSS delta values is maintained for each BS, as illustrated in Figure 9. The diagram displays the raw RSS values hovered above the window cells, with each entry shows the difference between the current and previous raw RSS value. The window size of 10 is used as a baseline configuration for the probation period in the proposed approach, ensuring that no handover occurs to any BS present in the MR for less than ten consecutive timestamps (i.e. probation period).

FIGURE 9. **Sliding window of 10 most recent signal rate of change.**

B. Probation Period Analysis and Mobility Impact

This subsection discussed a formal analysis of the probation period introduced through the sliding window mechanism in Section V.A. The probation period is defined by the number N of timestamps. The actual duration of this period depends on the sampling frequency f_s of RSS measurements, and can be expressed as:

$$T = \frac{N}{f_s} \tag{1}$$

where T is the total time of the probation period. In the proposed system, $N = 10$ timestamps are used as a baseline configuration. The spatial impact of the probation period depends on the UE velocity v. The distance travelled during the probation window can be expressed as:

$$D = v \cdot T \tag{2}$$

This relation indicates that the same number of timestamps corresponds to different spatial coverage depending on the mobility scenario.

For example, assuming a sampling frequency of $f_s = 10$ Hz, the probation period corresponds to $T = 1$ second. Under vehicular mobility conditions consistent with the simulation parameters in Table 5 (80–115 km/h), the UE travels approximately:

- 22.2 m at 80 km/h,
- 31.9 m at 115 km/h.

These values indicate that the probation period remains relatively short in time, but its spatial impact increases with velocity, which is particularly relevant for high-speed vehicular scenarios. The selection of N introduces a tradeoff between detection accuracy and handover latency. A larger value of N provides a longer sliding window, improving robustness against transient fluctuations and reducing false detections. However, it also increases the decision delay, which may negatively impact handover performance in high-speed scenarios.

In contrast, reducing N decreases latency and enables faster handover decisions but may increase sensitivity to

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

noise and short-term signal variations. Accordingly, the choice of $N = 10$ provides a balanced trade-off between robustness and responsiveness for typical vehicular scenarios.

C. Latency and Timing Feasibility for Real-Time Handover

Verification of zero-trust mechanisms must be completed within the time constraints imposed by handover decisions in order to prove their viability. The overall latency is primarily dominated by the probation period, as defined in (1), where $T = \frac{N}{f_s}$, which corresponds to approximately 1 second. In addition, the lightweight rule-based design of the trust-analysis pipeline results in negligible computational overhead. However, this bounded delay is acceptable for typical vehicular scenarios; it introduces a trade-off between detection reliability and responsiveness. In high-speed conditions (e.g., 115 km/h), a 1-second delay represents approximately 31.9 m of UE movement, which may affect handover performance in rapid radio conditions. Therefore, the development of adaptive tuning of the probation window based on mobility and network conditions is an important direction for future work.

D. Proposed Trust Analysis Algorithm

The proposed BS trust analysis is applied for every BS in the MR at each sample point, as shown in Figure 10. For any BS, either newly discovered or having re-entered the MR after previously exiting, the latest signal is read and inserted into the sliding window.

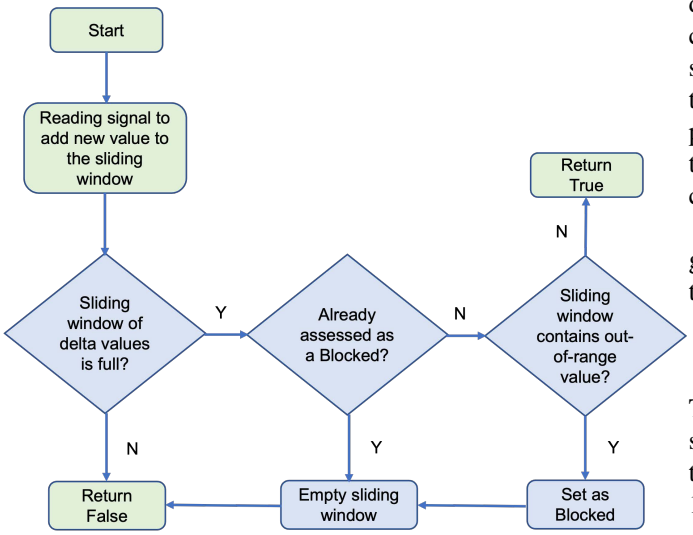

FIGURE 10. Base station trust analysis (calculated for each BS in the MR at each sample point).

The next RSS values are successively appended to the sliding window upon receipt and will continue until the probation period is complete. The procedure is repeated with every new incoming value.

E. Proposed Handover Protocol

Our suggested handover protocol improves the standard handover procedure by integrating the zero trust analysis model, proposed in Section V, thereby guaranteeing that any BS in the blocked state is never considered for handover, as shown in Figure 11. The currently serving BS remains connected while it is trusted, and no candidate exceeds the signal threshold. Handover then occurs to the strongest eligible candidate, therefore permanently excluding all blocked BS from connection.

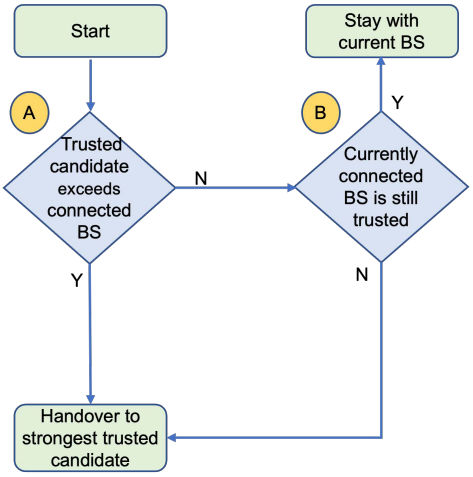

FIGURE 11. Base station handover protocol at each timestamp (assuming already connected to a BS)

Figure 12 displays the Karnaugh map for the final handover condition. Let A represents the condition that a trusted candidate base station exceeds the currently connected base station by the handover threshold, and let B represent that the currently connected base station remains trusted. In the proposed handover protocol, handover triggers when either the serving base station loses trust ($B = 0$) or a trusted candidate satisfies the threshold criteria ($A = 1$).

The Karnaugh map groups the cases where $B = 0$, which gives the term $\neg B$, and the cases where $A = 1$, which gives the term A. Hence, the simplified handover condition is:

$$HO = A \vee \neg B. \tag{3}$$

This Boolean expression is consistent with the decision flow shown in Figure 11, permitting a straightforward implementation in hardware or software, provided the trust analysis is 100% accurate.

VI. Experimental Results and Discussion

The experiment was run on the MATLAB platform on an Apple M4 Pro machine with 24 GB of RAM. The simulation framework generates radio information and realistic datasets, and also RSS measurements in a reconfigurable scenario featuring multiple LBSs and numerous RBSs. Employing radio propagation models, it creates MRs that closely replicate

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

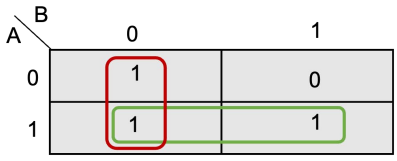

FIGURE 12. Karnaugh map for the final handover decision, showing the simplified logic $HO = A \vee \neg B$, where A represents the threshold condition and B indicates the trust status of the serving base station.

those obtained from real-world test. Our experiments show that a dataset that would represent a 20-minute drive test can be obtained in only 12 seconds of simulation. The simulation parameters are presented in Table 5.

TABLE 5. Simulation Parameters for the RBS Attack Scenario

Parameter	Value	Parameter	Value
Vehicle Speed	80–115 km/h	Number of RBS	6 / 18 / 90
Frequency	3.8 GHz	Road Width	50 m
RBS transmit Power	1 W	Road Length	22,500 m
Transmit PowerBS	10 W	RBS Gain	15 dBi
Number of BS	30 / 90 / 500	BS Gain	1 dBi

Our research experiments generate different datasets containing both malicious and legal Bayesian statistics. Various road lengths and BS/RBS positions/densities are included in the simulations. The dataset and simulation code are available on GitHub [31]. The received signal is computed per second while the UE, in this case, a platoon's lead vehicle, is within the BSs' range. Three datasets of varying sizes were constructed, as indicated in Table 6. For example, in the first dataset, we replicate a 500-kilometre road with 30000 timestamps, 90 valid BSs, and 18 rogue BSs. Details about the three datasets are provided.

TABLE 6. Simulation Parameters for Three Datasets

Dataset	LBS/RBS	Road Length(km)	Timestamp(s)
90LBS–18RBS	90/18	500	30,000
500LBS–90RBS	500/90	400	170,000
1000LBS–180RBS	1000/180	5000	225,000

Table 7 provides an illustrative excerpt of the proposed handover protocol. For feasible readability, only fine columns of the measurement dataframe are shown: the timestamp, RSS, and the corresponding RoCH values for both a BS and an RBS. This excerpt underscores the pivot role of the probation period, revealing that measurements acquired immediately before handover are essential in assessing the trustworthiness of candidate BSs.

The legitimate BS initially acts as a serving gNodeB until timestamp t-11, at which point the RBS first enters the MR.

TABLE 7. An example of handover protocol data snippet

Timestamp	BS	RBS	RoCHBS	RoCHRBS
t-12	-71.313	-900	0.24	0
t-11	-71.555	-87.09	0.13	0
t-10	-71.422	-82.027	0.6	5.59
t-9	-72.024	-76.442	0.94	5.49
t-8	-72.963	-70.956	0.71	4.79
t-7	-73.671	-66.167	0.14	0.27
t-6	-73.527	-66.44	0.11	1.55
		⋮		
t-2	-73.918	-67	0.16	0.12
t-1	-74.076	-67.121	0.26	1.08
t	-74.331	-66.039	0.51	1.73

As shown in the table, the RBS appears to exhibit normal behaviour from timestamp t-7 to the handover moment at t (highlighted in red). No anomalies are observed within this period; however, looking closely at the period from t-10 to t-8 (highlighted by the blue box), the increased RoCH suggests rogue-like behaviour, and requires the RBS to be assigned to the blocked state.

Had the proposed handover protocol not been implemented, handover to the RBS would have occurred at timestamp t-7. This case study underscores the critical importance of continuous monitoring for robust defence against RBS threats. Consequently, rogue-behaviour analysis must be performed at each sampling time point, irrespective of whether it remains within the probation period or has already moved to the candidate state. Analysis of successive signal level differences indicates that RBS detection is relatively straightforward. When these differences remain small, the recent samples closely align with the initial values of the sliding window, reflecting the steady signal growth expected from a legitimate BS. In contrast, a large difference indicates that the most recent RSS value markedly exceeds the intial value, signifying the rapid escalation characteristic of RBS behaviour.

Figure 13 shows several cases illustrating the signal behaviour under investigation. In the compiled dataset, each row presents the initial ten MR readings throughout a candidate base station's probation period. The first column specifies the serving BS, the subsequent ten columns detail its RSS measurements at successive timestamps, and the rightmost column reports the absolute difference between the average RSS over the first three timestamps and that over the final three timestamps. This metric, derived directly from experimental parameter settings and observed results, is expressed as:

$$\begin{aligned}\text{Ave_Chg} = \big|\, &\text{AVG}\big(RSS(ts_1 : ts_3)\big) \\ &- \text{AVG}\big(RSS(ts_8 : ts_{10})\big)\,\big| \end{aligned} \tag{4}$$

Legitimate BSs are represented by brown-colored rows, ranging from a minor average change of $\text{Ave_Chg} =$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

0.334 (light-brown) to a considerable average change of Ave_Chg = 2.936 (dark-brown). Blue-colored rows, in contrast, denote RBSs, ranging from a small average change (Ave_Chg = 0.170, light-blue) to a large average change (Ave_Chg = 6.479, dark-blue). The two classes are readily distinguishable, as the average change for the two groups lies in clearly separable ranges. Experimental results show that the Ave_Chg remains below 4 for LBSs and exceeds 4 for RBSs.

BS(i)	ts1	ts2	ts3	ts4	ts5	ts6	ts7	ts8	ts9	ts10	Ave_Chg	
LBS1	-82.34	-82.379	-82.694	-83.053	-82.66	-81.749	-82.29	-82.518	-82.993	-82.905	0.334	
LBS2	-81.356	-81.232	-80.788	-81.363	-81.25	-81.294	-81.024	-81.361	-81.562	-81.534	0.360	LBS
LBS3	-82.562	-82.542	-82.342	-82.394	-81.965	-82.06	-80.483	-79.613	-79.774	-79.952	2.702	
LBS4	-84.216	-83.137	-82.553	-82.651	-82.516	-82.415	-81.871	-80.607	-80.583	-79.907	2.936	
RBS1	-79.634	-74.974	-74.634	-74.587	-74.603	-74.506	-75.618	-76.059	-76.384	-76.289	0.170	
RBS2	-78.812	-74.487	-74.372	-75.386	-75.201	-74.911	-75.64	-76.202	-75.929	-76.224	0.228	RBS
RBS3	-79.401	-74.272	-68.775	-68.632	-68.887	-67.821	-68.883	-69.4	-69.036	-69.533	4.826	
RBS4	-80.627	-75.622	-70.398	-70.321	-69.167	-68.891	-68.952	-68.934	-69.077	-69.198	6.479	

FIGURE 13. Big and tiny jump in received signal for rogue agents.

However, some scenarios exhibit opposite behaviour. In case of minor differences, the recent RSS samples closely align with the value recorded at the start of the sliding window, indicating a gradual signal increase that can originate from either LBS or an RBS, as illustrated in Figure 13. In these instances, it is more difficult to distinguish the light-blue rows of rogue agents from the dark-brown rows of legitimate BS, since the average change of LBS approaches 3, while that for RBSs remains below 1. The figure further shows that the average difference for RBS samples is lower than for LBS samples, thereby presenting a significant classification challenge.

Figure 13 demonstrates that the majority of instances are readily classifiable, since a substantial RSS increase within the probation window reliably provide a clear indicator that the signal originate from an RBS rather than an LBS. However, in more intricate propagation environments, a direct comparison of signal strengths across the window proves insufficient for accurate classification, therefore demanding alternative classification techniques. The examined dataset originates from deliberately challenging conditions designed to expose specific edge cases in which the rule-based detection approach results in misclassification, revealing the limitation of the proposed approach and underscoring the need for supplementary or alternative techniques, such as adaptive threshold, anomaly detection [32], or ML classifiers, to achieve robust performance across the full spectrum of real-world scenarios.

The trust analysis model inspects RSS traces to detect signal spikes and classify the associated base stations as rogue. While the model exhibited robust performance on the different scenarios, it encountered limitations in more complex environments, where the rule-based technique produced misclassifications. Although the preceding illustration involved an RBS with a steep RoCH rise for detection, certain rogue agents may generate slower signal ramps that remain below the threshold. Moreover, the RoCH decision threshold is scenario-based in real-world conditions, influenced by BS transmit power, platoon velocity, road proximity, and other propagation factors. In high-density urban scenarios, multipath fading could mimic RoCH spikes, resulting in higher FNs.

The proposed RBS detection mechanism demonstrates strong performance across multiple datasets. For several examples in terms of the dataset with 90 BSs and 18 RBS as well as the 500LBS-90RBS dataset, it attains 98% accuracy with FN=7, defined as the instances in which rogue agents were erroneously categorized as legitimate. To further validate scalability, an additional experiment was performed on a substantially larger dataset consisting of 1000 LBS and 180 RBS with only 14 misclassifications. Despite these favourable outcomes, the method is not flawless. Consequently, an alternative ML solution is under active exploration. A principal challenge remains ensuring that the ML technique achieves simultaneously superior accuracy while satisfying the real-time latency requirements of live 5G deployments.

A. RoCH Threshold Selection and Sensitivity Analysis

The RoCH threshold plays an important role in balancing detection sensitivity and robustness against false alarms. In practical deployments, the optimal threshold value may vary depending on the radio environment, user mobility, and signal variability.

In general, a lower threshold increases sensitivity to quick signal changes and may improve detection of RBSs, but it can also increase FPs in highly dynamic environments. Conversely, a higher threshold reduces false alarms but may delay or miss detection when the signal deviation is small. This trade-off highlights the importance of selecting an appropriate threshold that balances detection accuracy and operational stability. In practice, a moderate threshold value provides a suitable compromise for real-time deployment at the gNodeB.

To further improve adaptability, future work will investigate ML approaches for dynamic threshold selection. For example, supervised learning models can be trained to classify normal and anomalous signal patterns, while unsupervised anomaly detection methods can identify deviations without labeled data. Such approaches can enable adaptive thresholding that responds to changing network conditions in real time. However, these methods introduce additional computational complexity and require training data, which may limit their immediate deployment in latency-sensitive handover scenarios. Therefore, the proposed rule-based threshold provides a practical baseline, while ML-based extensions provide a promising direction for enhanced robustness [33],

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

[34]. Given recent advances in fog-computing architectures for real-time security [35] and ML-based anomaly detection in IoT networks, we also plan to explore hybrid rule-ML models with adaptive RoCH thresholds.

VII. Threats to Validity

This paper relies on simulation-based evaluation, so several threats to validity should be acknowledged.

Internal validity. The RoCH-based rule and threshold of 3.17 dB, as well as a 10-timestamp probation period, were derived from the generated datasets. Although the sliding-window mechanism is deterministic and reproducible, non-modeled noise (i.e., sudden channel fading that is not captured by the propagation model) may affect classification. Our approach mitigated this problem by testing three dataset scales (90–1000 LBS) and stating false-positive reports explicitly.

External validity. Results are based on vehicular platooning scenarios with variant speeds (80–115 km/h) and synthetic radio propagation. Generalisation to dense urban environments, pedestrian UEs, or real 5G deployments (with dynamic power control and live beamforming) is limited. While the datasets are realistic in accordance with prior work [25], field trials will be needed for full validation.

Construct validity. The rogue label is made operational via sharp spikes in RoCH. Adaptive power ramping, for example, is a more sophisticated way of avoiding detection. Legitimate gradual rises (e.g., RBSs that mimic legitimate gradual rises) could evade detection. This is something we explicitly discuss, and we propose extending it with ML in the future. The future work proposes ML extensions that address this explicit concern.

Conclusion validity. The datasets are deterministic simulations, so there are no formal hypothesis testing or confidence intervals reported. The statistical claims (98% accuracy with FN=14 on the largest dataset) are descriptive and not inferential; therefore, no formal hypothesis testing or confidence interval reports are provided. The data generator produces consistent trends when it is run again using different random seeds; however, the results could differ with different propagation libraries. Overall, by making the simulation code and datasets publicly available [31] and outlining all assumptions explicitly, threats are mitigated. As future work, we will use real-world testbed validation and hybrid ML-rule techniques to address them [36].

VIII. Conclusion and Future Work

This work proposed a novel RBS detection system comprising a BS probation period feature, an extended handover protocol, and a zero trust analysis method. The RBS detector is implemented at the gNodeB, where suspected RBSs are tagged by assignment to the blocked state and thereby excluded from handover consideration. The initial zero trust analysis employs a rule-based approach that focuses on RoCH value patterns throughout the probation period, during which the BS remains ineligible for handover. The zero trust analysis model performs a numerical evaluation of the data to detect significant jumps in received signal from a BS and flag them as rogue. Although the model performed effectively across diverse scenarios, the rule-based approach produced misclassification in certain complex cases. Whereas the previous example featured an RBS with a sufficiently steep RoCH rise for detection, some rogue agents may exhibit more gradual spikes that evade identification. Furthermore, the RoCh threshold is scenario-dependent in real-world conditions, varying with BS signal power, platoon speed, location, and other factors affecting signal levels.

The RBS Detection system, integrated with the zero trust rule-based protocol, performs well. The accuracy is about 0.98, with 7 instances of RBS incorrectly classified as legitimate, and the FN for big data is 14.

As future work, an AI approach will be investigated to integrate ML for adaptive RoCh thresholds, addressing edge cases like low pike RBSs. Key challenges include ensuring that the ML techniques achieve substantially higher accuracy while remaining fast enough to support real-time classification. Given progress in fog computing for real-time security and ML-based IoT anomaly detection, we also plan to explore hybrid rule-ML models using adaptive RoCH thresholds. In addition, another plan is to suggest O-RAN for programmable gNodeBs or 6G AI-native extensions.

REFERENCES

[1] X. Lin and N. Lee, *5G and beyond: Fundamentals and standards*. Springer, 2021.

[2] C. Fiandrino, D. Martínez-Villanueva, and J. Widmer, "A study on 5g performance and fast conditional handover for public transit systems," *Comput Commun*, vol. 209, pp. 499–511, 2023.

[3] 3rd Generation Partnership Project (3GPP), "Evolved universal terrestrial radio access network," 3GPP, Tech. Rep. TS 36.401, 2022, accessed: Jan. 2026.

[4] ——, "Study on 5g security enhancement against false base stations (fbs)," 3GPP, Tech. Rep. TR 33.809, v1.0.0, 2023, accessed: Jan. 2026.

[5] B. Babb and M. Pruett, "Fam. court rev." *Fam. Court Rev.*, vol. 57, p. 293, 2019.

[6] N. I. of Standards and Technology, "Zero trust architecture," NIST, Tech. Rep. SP 800-207 (with 2025 Addendum for 5G Applications), 2020/2025, accessed: January 19, 2026. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[7] P. K. Nakarmi, M. A. Ersoy, E. U. Soykan, and K. Norrman, "Murat: Multi-rat false base station detector," *arXiv preprint arXiv:2102.08780*, 2021.

[8] 3rd Generation Partnership Project (3GPP), "Nr and ng-ran overall description," 3GPP, Tech. Rep. TR 38.300, 2021, accessed: Feb. 2026.

[9] R. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5g specifications," *IEEE Access*, vol. 7, pp. 24 956–24 963, 2019.

[10] M. Saedi, A. Moore, P. Perry, M.Shojafar, H. Ullah, J. Synnott, R. Brown, and I.Herwono, "Generation of realistic signal strength measurements for a 5g rogue base station attack scenario," in *IEEE Conference on Communications and Network Security (CNS)*, 2020, pp. 1–7.

[11] Z. Li, W. Wang, C. Wilson, J. Chen, C. Qian, T. Jung, L. Zhang, K. Liu, X. Li, and Y. Liu, "Fbs-radar: Uncovering fake base stations at scale in the wild," *NDSS Symposium*, 2017.

[12] S. Steig, A. Aarnes, T. V. Do, and H. Nguyen, "A network based imsi catcher detection," 2016, pp. 1–6.

[13] A. I. et al., "Anomaly detection against fake base station threats using machine learning," *J. Cybersecur. Priv.*, vol. 5, p. 94, 2025.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

[14] S. Steig, A. Aarnes, T. Van Do, and H. T. Nguyen, "A network based imsi catcher detection," in *2016 6th International Conference on IT Convergence and Security (ICITCS)*. IEEE, 2016, pp. 1–6.
[15] S. et al., "Network-based rogue base station detection in 5g," *IEEE Conf.*, 2021.
[16] M. Mahyoub, A. AbdulGhaffar, E. Alalade, E. Ndubisi, and A. Matrawy, "Security analysis of critical 5g interfaces," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 4, pp. 2382–2410, 2024.
[17] Z. Zhuang, X. Ji, T. Zhang, J. Zhang, W. Xu, Z. Li, and Y. Liu, "Fbsleuth: Fake base station forensics via radio frequency fingerprinting," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, 2018, pp. 261–272.
[18] I.-H. Liu, H.-H. Chen, B.-H. Tang, and J.-S. Li, "Rogue base station detection in industrial internet of things." *Sensors & Materials*, vol. 37, 2025.
[19] Y. Ullah, M. B. Roslee, S. M. Mitani, S. A. Khan, and M. H. Jusoh, "A survey on handover and mobility management in 5g hetnets: current state, challenges, and future directions," *Sensors*, vol. 23, no. 11, p. 5081, 2023.
[20] B. Zhang, P. Hu, A. A. Azirani, M. A. Salahuddin, D. Barradas, N. Limam, and R. Boutaba, "Secure and efficient group handover protocol in 5g non-terrestrial networks," in *ICC 2024-IEEE International Conference on Communications*. IEEE, 2024, pp. 5063–5068.
[21] T. H. Sulaiman and H. S. Al-Raweshidy, "Predictive handover mechanism for seamless mobility in 5g and beyond networks," *IET Communications*, vol. 19, no. 1, p. e12878, 2025.
[22] R. Kabre and E. R. Team, "Protect mission-critical networks with ericsson security manager: Behavior-based detection in 5g," 2025, accessed: January 19, 2026; Focuses on zero trust-inspired security for handover and RBS threats in mission-critical 5G environments. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/network-design-and-optimization-reports/securing-5g-networks-for-mission-critical-markets
[23] K. M. et al., "Gotta detect 'em all: Fake base station and multi-step attack detection in cellular networks," in *USENIX Security*, 2025. [Online]. Available: https://www.usenix.org/system/files/usenixsecurity25-mubasshir.pdf
[24] A. Shaik, S. Park, R. Borgaonkar, and J. Seifert, "On the impact of rogue base stations in 4g/lte self organizing networks," in *WiSec 2018 - Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2018, pp. 75–86.
[25] M. Saedi, A. Moore, and P. Perry, "Synthetic generation of realistic signal strength data to enable 5g rogue base station investigation in vehicular platooning," *Applied Sciences*, vol. 12, 2022.
[26] H. Kalbkhani, S. Yousefi, and M. Shayesteh, "Adaptive handover algorithm in heterogeneous femtocellular networks based on received signal strength and signal-to-interference-plus-noise ratio prediction," *IET Communications*, vol. 8, pp. 3061–3071, 2014.
[27] L. Arnold, M. Hollick, and J. Classen, "Catch you cause i can: busting rogue base stations using cellguard and the apple cell location database," in *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*, 2024, pp. 613–629.
[28] J. Xu, V. Loscri, and R. Rouvoy, "Integrity under siege: A rogue gnodeb's manipulation of 5g network slice allocation," *arXiv preprint arXiv:2511.03312*, 2025.
[29] S. Sun, I. Abualhaol, G. Poitau, A. Esswie, and M. Repeta, "An ensemble approach for fake base station detection using temporal graph analysis and anomaly detection," in *2024 Wireless Telecommunications Symposium (WTS)*. IEEE, 2024, pp. 1–6.
[30] M. Harvanek, J. Bolcek, J. Kufa, L. Polak, M. Simka, and R. Marsalek, "Survey on 5g physical layer security threats and countermeasures," *Sensors (Basel, Switzerland)*, vol. 24, no. 17, p. 5523, 2024.
[31] M. Saedi, "Rbs-ml," https://github.com/mohammadmsaedi/RBS-ML, 2025, gitHub repository.
[32] R. Lamptey, M. Saedi, and V. Stankovic, "Machine-learning anomaly detection for early identification of ddos in smart home iot devices," in *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2025, pp. 105–110.
[33] R. Das and M. M. Inuwa, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on iot networks," *Internet of Things*, vol. 26, p. 101162, 2024.
[34] H. Ahmetoglu and R. Das, "A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions," *Internet of Things*, vol. 20, p. 100615, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S254266052200097X
[35] R. Das and M. M. Inuwa, "A review on fog computing: Issues, characteristics, challenges, and potential applications," *Telematics and Informatics Reports*, vol. 10, p. 100049, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772503023000099
[36] E. Nowroozi, Y. Habibi, A. B. Mughal, M. Saedi, and M. Jafari, *Enhancing Federated Learning Security: Cluster-Based Strategies to Counter GAN-Poisoned Attacks*. Cham: Springer Nature Switzerland, 2026, pp. 225–235. [Online]. Available: https://doi.org/10.1007/978-3-031-99447-0_16

Mohammad Saedi(M'19) was born in Kurdistan, Iran. He received the BEng (Hons) and MEng (Hons) degrees in computer engineering in Iran, and then the PhD degree in computer science with a focus on 5G network security from Ulster University, Belfast, U.K.

He was a Senior Lecturer in Computing at Sheffield Hallam University, Sheffield, U.K., and is currently a Lecturer and Assessment Lead in the Department of Computer Science at City St George's, University of London, London, U.K. Previously, he worked as a BTIIC researcher focused on secure communication over 5G networks and as a network security specialist in industry. He has been involved in various (BTIIC, EU, etc.) projects, e.g., as the Principal Investigator for the Pump Priming and Urban Vehicular Navigation System projects. He led multiple research projects, with expertise spanning 5G service platforms, mobile network security, computer networks, data science, cloud computing, V2X, IoT and AI/ML.

Dr. Saedi holds a Fellowship of the UKPSF from AdvanceHE, and also works as an Independent Assessor at Manchester Metropolitan University, where he chairs EPA sessions. He is a member of the British Computer Society, the IEEE Communications Society, the IEEE Vehicular Technology Society, and the IEEE Computer Society, and serves as a peer reviewer for *IEEE Transactions on Vehicular Technology*, *IEEE Transactions on Network and Service Management*, *IEEE Systems Journal*, *IEEE Access*, *IEEE CSR*, etc.

Adrian Moorewas awarded a first-class honours in BSc Computing (1987) and a PhD in Computer Graphics (1992), both from the University of Ulster. He is currently a Senior Lecturer in the School of Computing at Ulster where he specialises in teaching online applications development using full-stack architectures. Dr. Moore is a member of the Artificial Intelligence Research Centre at Ulster and a grant holder in the BT Ireland Innovation Centre, where he currently works on Autonomic IoT solutions.

Fehmi Jaafarreceived the Ph.D. degree from the Department of Computer Science, Université de Montréal, Montreal, QC, Canada.

He was a Postdoctoral Research Fellow at Queen's University, Kingston, ON, Canada, and at Polytechnique Montréal, Montreal, QC, Canada. He was also a Cybersecurity Researcher at the Computer Research Institute of Montreal (CRIM), Montreal, QC, Canada, and an Adjunct Assistant Professor at Concordia University of Edmonton, Edmonton, AB, Canada. He is currently the Director of the Research Chair on Cyber Defence and Protection of Personal Information (CybPro) and an Associate Professor at the Université du Québec à Chicoutimi, Chicoutimi, QC, Canada. He has established externally funded research programs in collaboration with Defence Canada, Safety Canada, NSERC, MITACS, industrial partners, and foreign universities. His research

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2026.3691214

interests include cybersecurity in the Internet of Things, protection of data and communications in distributed systems, and the application of ML techniques in cybersecurity.

Dr. Jaafar's research has been published in top venues in computer science, including *IEEE Transactions on Reliability* and *Springer Nature Computer Science*.

MD. ARAFATUR RAHMAN (Senior Member, IEEE) received the Ph.D. degree in electronics and telecommunications engineering from the University of Naples Federico II, Naples, Italy, in 2013. He has around 15 years of research and teaching experience in the domain of computer and communications engineering. Currently, he is a Reader in Cybersecurity with the School of Engineering, Computing and Mathematical Sciences, University of Wolverhampton, U.K. He was an Associate Professor with the Faculty of Computing, Universiti Malaysia Pahang. He was also a Postdoctoral Research Fellow with the University of Naples Federico II in 2014 and a Visiting Researcher with the Sapienza University of Rome in 2016.

He has co-authored around 150 publications in prestigious IEEE and Elsevier journals, such as *IEEE Transactions on Industrial Informatics*, *IEEE Transactions on Intelligent Transportation Systems*, *IEEE Transactions on Green Communications and Networking*, *IEEE Transactions on Services Computing*, *IEEE Communications Magazine*, JNCA (Elsevier), and FGCS (Elsevier); and conference publications such as *IEEE GLOBECOM* and *IEEE DASC*. His research interests include the Internet of Things (IoT), wireless communication networks, cognitive radio networks, 5G, vehicular communication, cyber-physical systems, big data, cloud-fog-edge computing, ML, and security.

He received the Higher Education Academy (HEA) Fellowship, U.K. He has served as a Patron, General Chair, Organizing Committee Member, Publicity Chair, Session Chair, Program Committee Member, and Technical Program Committee (TPC) member in several leading conferences worldwide (e.g., *IEEE GLOBECOM*, *IEEE DASC*, *IEEE iSCI*, and *IEEE ETCCE*) and journals. His name was listed in the World's Top 2% Scientists list released by Stanford University under the category of Citation Impact in a Single Calendar Year (2019–2021). He was endorsed by the Royal Academy of Engineering, U.K., as a Global Talent under the category of "Exceptional Talent" in 2022. He has served as a Specialty Chief Editor for IoT Theory and Fundamental Research (specialty section of *Frontiers in the Internet of Things*), an Advisory Board Member and Editor for *Computers* (MDPI), a Lead Guest Editor for *IEEE Access* and *Computers*, and an Associate Editor for *IEEE Access*.

Sujit Biswas is a blockchain researcher and academic with significant contributions to distributed ledger technologies. He is a Senior Lecturer (Associate Professor) in Cybersecurity and Programme Director of Cybersecurity in the Department of Computer Science at City St George's, University of London, UK. Prior to this role, he served as a Lecturer in Computer Science and Digital Technologies at University of East London, a Research Fellow in Blockchain and Artificial Intelligence at the Centre for Vision, Speech and Signal Processing (CVSSP), University of Surrey, and an Assistant Professor in Computer Science and Engineering at University of Dhaka, Bangladesh. He received his PhD in Computer Science and Technology from Beijing Institute of Technology, China. Dr. Biswas's research focuses on blockchain consensus mechanisms, scalability, privacy-preserving and trustworthy AI systems, and the integration of blockchain with federated learning and IoT/IoMT applications. His work has been published in leading international journals and conferences, including IEEE Internet of Things Journal, IEEE Transactions on Big Data, IEEE Transactions on Engineering Management, IEEE Transactions on Services Computing, Computer, and ACM Computing Surveys. He is currently serving as an Associate Editor of IEEE Transactions on Consumer Electronics, . In addition, he has organised and served as Guest Editor for multiple special issues in high-quality journals, including IEEE Transactions on Network Science and Engineering, Computer, MDPI Sensors, MDPI Electronics, and MDPI Mathematics. In addition to his research, Dr. Biswas is an experienced educator and mentor, teaching and supervising across blockchain, cybersecurity, federated learning, and machine learning. He is actively involved in multidisciplinary collaborations with industry, government, and international academic partners, aiming to translate cutting-edge research into real-world impact. His editorial interests align with high-quality, rigorous, and application-driven research in blockchain, distributed systems, and secure AI.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/