Evaluating Time-Bounded Defense Against RRC Relay in 5G Broadcast Messages

Yilu Dong
The Pennsylvania State University
University Park, PA, United States
yiludong@psu.edu

Tao Wan
CableLabs
Louisville, CO, United States
Carleton University
Ottawa, ON, Canada
t.wan@cablelabs.com

Tianwei Wu
The Pennsylvania State University
University Park, PA, United States
tvw5452@psu.edu

Syed Rafiul Hussain
The Pennsylvania State University
University Park, PA, United States
hussain1@psu.edu

Abstract

As 5G and future generations of mobile networks aim to provide faster and more secure wireless connections, 5G broadcast messages remain unprotected. Hence, a user device cannot verify the identity of a base station before establishing the connection and starting the registration procedure. This long-existing loophole enables various types of fake base station (FBS) attacks. To protect end-users from these attacks, a practical solution is to incorporate digital signatures to these broadcast messages. However, an FBS may also have the ability to relay a digitally signed broadcast message from a benign base station to bypass the protection. Considering that a relayed message needs extra time to reach a user device, a time-bounded defense mechanism can be used on top of the digital signature to offer replay protection. Although previous work proposed such a solution, none have implemented it or evaluated it against relay attacks. Hence, to evaluate the performance of our proposed digital signature scheme and the time-bounded defense, we implemented the solution against relay attacks using an open-source 5G system. Our results show that the overhead introduced is acceptable and that the time-bounded defense is effective against relay attacks.

CCS Concepts

• **Security and privacy → Mobile and wireless security**.

Keywords

5G; Wireless Security; Authentication Protocol; Defense Mechanism

ACM Reference Format:
Yilu Dong, Tao Wan, Tianwei Wu, and Syed Rafiul Hussain. 2025. Evaluating Time-Bounded Defense Against RRC Relay in 5G Broadcast Messages. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '25), June 30–July 3, 2025, Arlington, VA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3734477.3734485

WiSec '25, Arlington, VA, USA

ACM ISBN 979-8-4007-1530-3/25/06
https://doi.org/10.1145/3734477.3734485

1 Introduction

Throughout the evolution of mobile networks—spanning from 2G to 5G—numerous vulnerabilities and attacks emerged [8, 15, 16, 18, 23, 25–28, 31]. For example, an attacker can send an SMS message with any phone number to phish a user or to track the user by capturing the victim device's permanent identifier, the International Mobile Subscriber Identity (IMSI). Although the current generation, i.e., 5G systems are now widely deployed around the world, offering higher throughput and lower latency, very few security measures have been taken to prevent such attacks. For example, 5G specifications recommend that SMS can now be encrypted and integrity-protected over the air. It also introduced the Subscription Concealed Identifier (SUCI) to encrypt the IMSI over the air, preventing the illegitimate exposure of sensitive information. However, the root cause behind FBS attacks unfortunately remains unresolved, i.e., a user device cannot authenticate a base station before connecting to it.

As most attacks require an attacker to force the user devices to connect to an FBS, it is important to understand the long-inherited cell selection procedure in cellular networks. The cell selection procedure is carried over from 4G to 5G with no significant changes. A user device (e.g., a mobile phone) needs to select and switch between different base stations during movement to keep network access. To select a suitable cell, a user device first needs to receive the `Master Information Block` (MIB) and the `System Information Block Type1` (SIB1) messages broadcasted from the nearby base stations. With an FBS broadcasting the same messages with a higher signal strength, a user device is duped to connect to the FBS inadvertently.

If a user device can verify the authenticity of a base station before connecting, it can avoid most, if not all, FBS attacks. There are a few existing works [10, 17, 29] that proposed cryptographic solutions for base station authentication and suggested a time-bounded defense against relay attackers. However, none of the works implemented relay attacks and evaluated the effectiveness of the proposed time-bounded solution against these attacks. Moreover, there is no existing work that implemented and evaluated such scheme on a 5G base station. Without sufficient evaluation and protection of replay attacks, those proposed solutions are not considered secure.

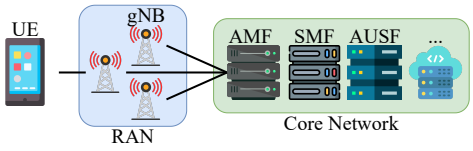

Figure 1: 5G System Overview

To address these challenges, we develop a Public Key Infrastructure (PKI)-based authentication scheme with short-lived signatures and timestamp verification for replay protection. Our scheme requires a minimal amount of change in specification and implementations, and it is fully backward-compatible with the existing specifications. We also developed a control-plane protocol relay to simulate the attack scenario. The results show that it takes 3 milliseconds (ms) and 7ms in average for a user device to receive a broadcast message from a legitimate base station and a relay FBS, respectively, demonstrating that a user device can use delay to detect relay attacks. Our results provide a reference to guide the design and implementation of future specifications on broadcast message authentication schemes. To summarize, in this paper, we make the following contributions:

- We developed a PKI-based authentication scheme using short-lived keys to authenticate broadcast messages in 5G systems.
- We implemented an RRC layer relay for 5G SIB1 messages.
- We evaluated the performance of our authentication scheme with SDR devices and the effectiveness of time-bounded defense against relay attacks.
- We submitted our solution to the Third-Generation Partnership Project (3GPP)—the standard body for cellular networks. 3GPP has accepted it as a candidate for mitigating fake base stations in Technical Report (TR) 33.809 [5] Solution 27.

Our research demonstrates that the PKI-based authentication scheme with the time-bounded defense mechanism is efficient and effective against fake base station attacks.

2 Background

2.1 Overview of 5G System

The 5G system comprises three key components: User Equipment (UE), Radio Access Network (RAN), and Core Network (CN), as shown in Figure 1. UEs, such as smartphones, are end-user devices that connect to the 5G network via the 5G radio interface. The RAN consists of a network of base stations, referred to as gNodeB (gNB) in 5G, which provide radio access to UEs and facilitate seamless mobility by enabling handovers between base stations. The gNB establishes connections with the Access and Mobility Management Function (AMF) in the core network. The CN is divided into multiple network functions responsible for UE authentication, mobility management, and session management, ensuring efficient and secure network operations.

2.2 5G Broadcasting Messages

Before connecting to a 5G base station, the UE must obtain the base station's configuration over-the-air from broadcast messages. As illustrated in Figure 2, a gNB transmits the `Master Information Block` (MIB) and various `System Information Block` (SIB) messages to the UE. The MIB and SIB1 messages together constitute the

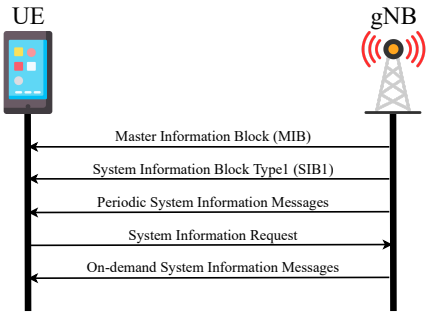

Figure 2: 5G Broadcast Message Procedure

Minimum System Information (MSI), which the UE must receive before establishing a connection with the gNB. Additionally, other System Information (SI) messages may be broadcast to all UEs or requested individually by a UE during the registration procedure [4]. According to 3GPP Technical Specification (TS) 38.213 [3], the gNB broadcasts the MIB every 80 milliseconds and SIB messages every 160 milliseconds. The SIB1 message is also periodically rebroadcast within the 160-millisecond interval, typically every 20 milliseconds, as configured by the gNB. Since this process occurs before mutual authentication between the UE and the network, these broadcast messages remain unprotected. Consequently, a fake base station can fabricate or relay these messages to deceive the UE into establishing a connection.

2.3 Threat Model

For this, attackers set up FBS using specialized radio equipment or software-defined radios (SDRs) to impersonate legitimate base stations and lure nearby users. They can launch various attacks through FBS, including denial-of-service (DoS) [15, 16, 25, 26, 28], downgrade [15, 16, 27, 28], battery depletion [15, 16, 28], information leakage attacks [8, 15, 18, 23, 31], location tracking attacks [8, 23, 31], and fingerprinting attacks [23, 25, 31]. Additionally, FBS attackers can establish relays to replay messages from legitimate gNB to UE, further complicating detection and mitigation efforts.

We consider that an FBS attacker can transmit 5G broadcast messages with higher power than a legitimate gNB. After the UE tries to connect to the FBS, the FBS can send and receive messages to/from the UE. In addition, the attacker can set an RRC layer relay which enables itself to decode, modify, and re-encode messages from a legitimate gNB before transmitting them to the UE. We only consider the RRC layer (Layer 3) relays because although lower-layer (Layer 1 and Layer 2) relays may introduce less delay, they can only forward messages blindly, making it challenging for attackers to selectively replay or modify message content. With an RRC relay, an FBS attacker can identify MIB and SIB1 messages originating from legitimate base stations, extract their contents, and modify them to align with the physical parameters of the FBS. This manipulation increases the likelihood of victim UEs attempting to establish a connection with the attacker-controlled base station.

2.4 Existing Approaches to Prevent FBSs

The fake base station (FBS) problem has persisted since the inception of cellular network technologies, and various solutions have been proposed to mitigate or resolve it. Some approaches focus on

detecting FBSs using online base station databases or message signatures. However, database-based solutions [1, 6, 9, 12, 30, 32] fail to detect FBSs that relay system information messages, as the FBS can replicate the legitimate base station's cell identity and operate in the same location as the station it impersonates. Signature-based detection methods [11, 21] analyze control-plane messages exchanged between the UE and gNB to identify anomalies. However, some attacks occur as soon as the UE receives these messages, meaning detection may come too late to prevent the attack.

An alternative approach is to use cryptographic authentication mechanisms [10, 17, 29] for these unprotected broadcast messages. Time-bounded defense mechanisms are included in these solutions to prevent relay attacks, leveraging the fact that relayed messages introduce additional end-to-end latency. Hence, the UE should theoretically be able to distinguish original messages from relayed ones. While this claim is compelling, no prior work has experimentally validated its practicality. Our research aims to bridge this gap by implementing and evaluating the effectiveness of a time-bounded defense against relay-based FBS attacks.

3 Protecting System Information

We developed a short-lived public key-based solution, along with time-bounded replay protection, to protect 5G system information. Our solution is accepted by 3GPP as a candidate for mitigating faked base stations in 3GPP Technical Report (TR) 33.809 [5] Solution 27.

3.1 Short-lived Asymmetric Key-Based Solution

An overview of our proposed protocol is provided in Figure 3. In the figure, we use K^+ to denote the public key and Sign(m) to denote the signature of message m. A new network function, the Digital Signing network Function (DSnF) [14], is introduced in the CN, to serve as a trust anchor. DSnF signs the public key of gNB, and gNB signs its SI, then broadcasts the public keys and signatures to the UE. The following sections explain the procedure in detail.

3.1.1 Provision root of trust. We opt to use a PKI-based solution to verify the authenticity of the 5G broadcast messages. Hence, a root of trust must be provided inside the UE. The operator should provision the root certificate used in the scheme inside the USIM on the UE. The certificate here can be the public key of DSnF or the public key of a higher entity in the certificate chain, which enables the UE to verify the signature generated by DSnF. Hence, the chain of trust can be expanded to multiple levels above the DSnF.

In roaming cases, the UE can download the trust anchor certificates of the visited operators through its home operator or other trusted sources, e.g., Global Systems for Mobile Communication Association (GSMA) before establishing a connection.

3.1.2 Base station registration. To establish the chain of trust, the gNB needs to generate its public-private key pair and send its public key to the DSnF to obtain a signature. K^+_{gNB} is sent together with $\text{Sign}_{gNB}(K^+_{gNB})$ to prove the gNB owns the public-private key pair. For this, we introduce a new NGAP message to send the message through the N2 interface between gNB and the AMF. Then the AMF forwards this message to DSnF. The DSnF signs K^+_{gNB} and returns the signature to gNB. After gNB receives $\text{Sign}_{DSnF}(K^+_{gNB})$, it uses the signature to prove itself as a valid base station to the UE.

Since the gNBs are deployed in the field, the keys generated inside the gNB have a higher risk of being leaked or compromised. We design the gNB key pairs as short-lived to avoid overhead from certificate revocation. That means the key should expire in a short interval. The expiration time can be set within 10 minutes to 24 hours, depending on different base station configurations and adversary levels. The gNB should generate a new pair of keys and request a new signature from DSnF when it first registers to the core network or the last key pair expires. The advantage of having DSnF instead of a Certification Authority (CA) signing gNB public key is to reduce the need for a new interface from gNB to CA for ongoing key renewal. In addition, most CAs in mobile networks are kept offline to reduce security risks, making it impractical to renew key signing in real-time. This is similar to the idea of delegated credentials (RFC9345 [7]).

3.1.3 Signature generation in gNB. After the key pair and the signature are ready on the gNB side, the gNB can use its private key to sign the system information messages. We choose to sign MIB, SIB1, and the timestamp of the SIB1 message sent together. Due to the limited size of the MIB, the signature cannot be embedded directly within it. However, the content of the MIB remains unchanged during the 80ms period, the UE can collect MIB and SIB together, then verify them before initiating the connection. The timestamp must also be protected, otherwise, an attacker may decode the message and be able to replay the message with a more recent timestamp to pass the freshness test, making the whole scheme useless. By signing MIB, SIB1, and the timestamp together, we also reduce the bytes sent over the air. The gNB adds the timestamp and generated signature to the SIB1 message and refreshes them before sending each new SIB1 message.

Since the SIB1 message already contains the necessary information about the gNB configuration, it may not have enough space to carry K^+_{gNB} and $\text{Sign}_{DsnF}(K^+_{gNB})$ within its maximum length (372 bytes). To address this limitation, we introduce a new SIB message, denoted as *SIBx*, to carry these messages. SIBx can be deployed in two ways. First, the gNB can broadcast SIBx periodically, similar to SIB1. This allows UEs to acquire and cache the gNB's public key and signature prior to initiating a connection. Alternatively, the UE can explicitly request SIBx as an on-demand SIB from the gNB during the initial access procedure. The extra space in SIBx can be used to transfer longer public keys and signatures with better security levels.

3.1.4 Base station verification in UE. After the UE receives MIB, SIB1, and SIBx messages from the gNB, it can verify the authenticity of the base station. First, it verifies the timestamp comes with the SIB1 message. If the time difference between the current time and the SIB1 time is greater than a threshold t, the message might be replayed by an attacker. The threshold t can be determined based on the configuration of the base station and the distance between the UE and the gNB. After the timestamp passed the verification, the UE needs to verify $\text{Sign}_{DSnF}(K^+_{gNB})$ using K^+_{DSnF} provisioned in the USIM. If the verification is successful, the UE can trust the public key sent from the gNB. Then, the UE verifies Sign_{gNB}(MIB+SIB1+TS) using K^+_{gNB} to decide if the system information received is valid.

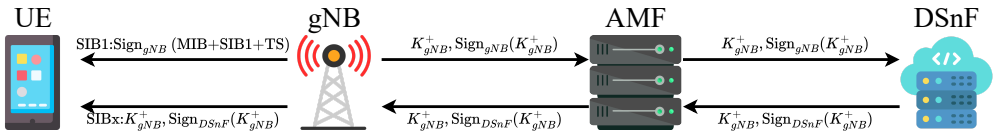

Figure 3: PKI-based Authentication Scheme

After successfully verifying all the messages, the UE can determine that the base station is legitimate and start a connection.

4 Evaluation

4.1 Testbed Setup

We implemented our solution based on OpenAirInterface (OAI) [22], an open-source implementation of 5G gNodeB, UE, and core network. All the experiments were done on an AMD Ryzen 7 5800X desktop with 32GB DDR4 memory, running Ubuntu 22.04.

Core network setup. We run each component of the 5G core network in Docker containers. To provide the signature functionality, we also run the Digital Signing Network Function (DSnF) [14] in a Docker container along with other network functions.

gNB setup. We run OAI gNB on USRP B210s [2]. We modified the gNB implementation to implement our proposed solution. We also incorporated the new SIB sent by the gNB to the UE.

UE setup. Similar to the gNB, we run the OAI UE on USRP B210s and modify the implementation to support the proposed protocol.

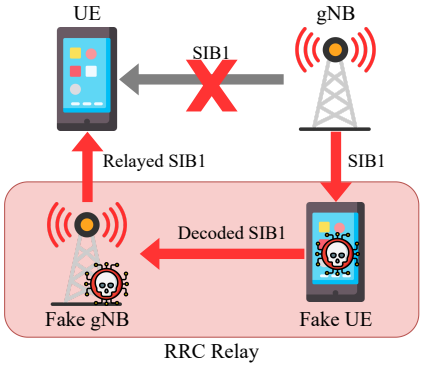

Figure 4: RRC Relay Workflow

RRC relay setup. To demonstrate and evaluate the effectiveness of our time-bounded defense mechanism, we have developed an RRC layer broadcast message relay, as illustrated in Figure 4. The relay consists of two components: a UE and a gNB controlled by the attacker. Similar to the benign UE and gNB, we also implement the relay based on OAI and USRP B210. The UE captures broadcast messages from a legitimate gNB, decodes them, and forwards them to the fake gNB. The attacker can then re-encode and transmit the altered messages from the fake gNB to the victim UE. In this scenario, the FBS attacker masquerades as a legitimate nearby base station. Since the attacker operates within the same location and uses identical System Information parameters, existing location- and identity-based FBS detection methods [1, 6, 9, 12, 30, 32] fail to detect its presence. However, the time-bounded defense mechanism described in the previous section effectively prevents the UE from connecting to such an attacker.

4.2 Performance of the Authentication Scheme

4.2.1 Overhead in bytes. Since our authentication scheme is implemented within a newly designated SIB, we can utilize the full SIB size of 372 bytes (2976 bits). Unlike approaches that rely on the limited remaining space in SIB1, our solution accommodates more secure cryptographic algorithms, such as ECDSA with the secp256k1 curve. In our implementation, we allocate 32 bytes (256 bits) for the private key, 33 bytes (257 bits) for the compressed public key, 64 bytes (512 bits) for the gNB signature, 64 bytes (512 bits) for the core network signature, and 8 bytes (64 bits) for the timestamp. Consequently, the additional overhead in SIB1 is 72 bytes and the total size of our new SIB is 97 bytes.

This implementation offers significant flexibility, allowing mobile network operators to select cryptographic algorithms based on their security requirements, provided they fit within the available SIB space. Additionally, the framework supports future advancements, enabling the integration of newly developed or more secure algorithms to enhance the overall security of broadcast message authentication in 5G networks.

4.2.2 Overhead in time. As shown in Table 1, the average signature generation time in our experiments is 1.55ms. Compared to the 20ms SIB transmission interval, this overhead is minimal. Moreover, since real-world gNBs are typically equipped with more powerful hardware than our desktop testbed, the actual computational overhead in the field may be even lower. To further optimize performance, we predict the transmission time of the next SIB and precompute its signature. This approach not only reduces computational overhead but also minimizes end-to-end delay, enhancing the practicality of our solution against RRC relay attacks.

The average signature verification time, which closely aligns with the processing time of the new SIB, is approximately 2 milliseconds. Notably, this is lower than the processing time of SIB1 (2.69 milliseconds). These results indicate that our authentication scheme can be integrated into UEs without introducing significant performance overhead, making it a viable solution.

Time (ms)	mean	median	stddev
signature gen	1.55	1.51	0.187
SIB1	2.69	4.52	2.297
New SIB	2.01	1.96	0.253

Table 1: Overhead introduced in our solution.

4.3 Effectiveness of the Time-Bounded Defense

4.3.1 Experiment setup. To get an accurate end-to-end delay from the gNB sending the SIB1 to the UE receiving the SIB1, we ran all the experiments on one single machine. Since the delay time is computed from the difference between the timestamp inside of the SIB and the machine time when this SIB message is received

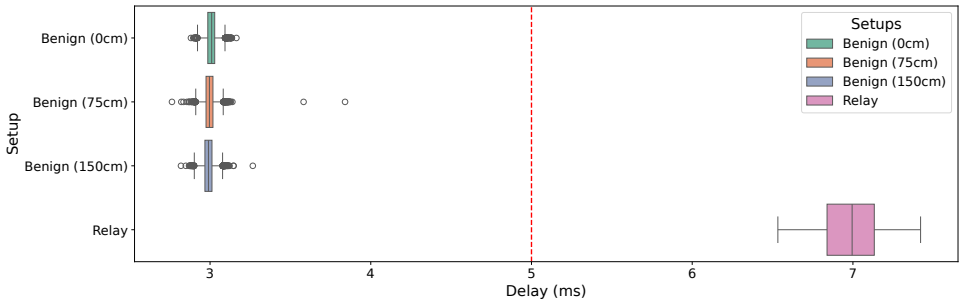

Figure 5: Delay Distribution by Setup

in the RRC layer, if we ran the experiment on different machines, the clock of the machines may not be perfectly synchronized and a sub-millisecond error may be introduced in our result.

We collect the end-to-end delay in 4 different setups. Among them, 3 experiments simulate the benign scenario, with the UE and the gNB placed in 0, 75, and 150 centimeters (cm). Here in the 0cm experiment, we place two USRP B210s right after each other. In the 75cm and 150cm experiments, we measure the distance between two USRP B210s to be the exact distance. Another experiment considers a relay attacker is present, a pair of benign UE and gNB, and a pair of fake UE and gNB are connected as the RRC relay shown in Figure 4. We measure the end-to-end delay of these setups for 30,000 messages and summarize the results. In the attack scenario, we place both the benign gNB-fake UE and the fake gNB-victim UE pair right after each other (0cm) to ensure the best possible signal quality and the smallest propagation delay between the parties. In addition, we transmit the decoded SIB1 message from the fake UE to the fake gNB using a UNIX domain socket, which should be faster than a TCP connection. If the attacker needs to transmit the data to a different machine using the Internet, even more delay will be introduced. Our setup favors the relay attacker and aims to demonstrate that the best-case scenario for the attacker can still be detected using the proposed time-bounded defense.

Time (ms)	max	min	mean	median	stddev
Benign (0cm)	3.164	2.881	3.009	3.010	0.030
Benign (75cm)	3.840	2.763	2.997	2.996	0.032
Benign (150cm)	3.266	2.819	2.990	2.990	0.032
Relay	7.421	6.533	6.986	6.995	0.178

Table 2: SIB reception time in benign and relayed scenarios.

4.3.2 Result and Analysis. Empirically, the relayed message will have twice the propagation delay as a benign message. As shown in Table 2, our results prove our theory. The mean and median reception time of the relayed SIB is more than twice that of the benign SIB. Figure 5 provides a clearer visualization of the delay distribution in different experiment setups. We observed no statistically significant difference in the delay measured from the three benign scenarios. The data follow a similar distribution, with the most data points around 3ms, indicating that the distance between the UE and gNB in our experiments makes a negligible impact on the result. The attack scenario is clearly separated from the benign experiments. The vertical line indicates our proposed threshold, 5ms. With the proposed threshold, no relayed SIB messages are accepted, and no benign SIB messages are rejected. That proves the effectiveness of the time-bounded defense solution.

4.4 Limitation of Our Experiments

Since commercial off-the-shelf (COTS) gNBs and UEs are closed-source, integrating our solution directly into these systems is not feasible. Therefore, we conducted our experiments using USRP B210 software-defined radios and the OAI software stack. While our results provide valuable insights, they may differ from those obtained in a commercial deployment with proprietary base station hardware and professional FBS equipment. Additionally, real-world UEs may have lower computational power than our desktop-based test environment; however, dedicated hardware accelerators in baseband processors could potentially offset this difference.

Furthermore, due to limitations in our lab equipment, we were unable to evaluate benign scenarios over extended distances or in varying environmental conditions (e.g., transmissions in high-noise environments). We recommend that a more comprehensive study be conducted before deploying this solution in commercial networks. Nevertheless, given that radio signals travel at the speed of light, the propagation delay for a signal to traverse 30 kilometers is only 0.1 milliseconds. Thus, under typical deployment conditions, the delay introduced by the distance between a UE and a legitimate gNB remains negligible. Despite these constraints, our results provide strong evidence supporting the feasibility of our proposed scheme.

5 Discussion

5.1 Time Synchronization

Signature freshness validation requires millisecond-level time synchronization between the UE and gNB. UEs typically obtain precise time from a Global Navigation Satellite System (GNSS) or a network-based protocol (e.g., Network Time Protocol (NTP)). However, an attacker can spoof the GNSS time, and the UE can only use NTP after connecting to the network. UE clock desynchronization, caused by events such as being powered off or attacks, can lead to the rejection of legitimate gNB signatures.

To address this, the UE can verify the consistency of timestamps obtained from multiple neighboring cells. By collecting timestamps from several gNBs and comparing them, the UE can distinguish between its own clock drift and inconsistencies among the received timestamps. If the timestamps from multiple legitimate gNBs are consistent relative to each other, despite a large divergence from the UE's local time, the UE can infer the correct time reference.

The introduction of malicious FBSs transforms this into a Byzantine fault problem [24]. Under the attack scenario, the timestamp consistency check remains effective. Reliable consistency can be achieved if over two-thirds of the received timestamp information originates from legitimate base stations, enabling the UE to disregard inconsistent information from malicious sources.

5.2 Defense Against Signal Injection Attacks

The solution discussed in this paper should efficiently prevent a UE from connecting to a fake base station that does not have access to the operator's core network. However, an attack can still happen if the attacker injects malicious messages, e.g., authentication or registration rejects, [13, 15, 16, 19, 20, 33] after the UE connects to a legitimate base station. We acknowledge that the solution presented in this paper cannot offer protection against these attacks. However, if we combine our solution with further protections, such as encrypting all post-authenticated communications between the UE and gNB, the UE will no longer accept attack-crafted messages. These protections are out of the scope of this work since they require a larger change in the protocol.

6 Conclusion

We implemented a practical PKI-based authentication scheme for securing 5G broadcast messages, incorporating a time-bounded defense mechanism. Our evaluation demonstrates that the proposed scheme effectively prevents the UE from connecting to a fake base station, even in the presence of an adversary capable of deploying an RRC relay to replay messages. Given the critical importance of this protection, we encourage standardization bodies to consider integrating such mechanisms into future specifications.

Acknowledgments

This work has been supported by the NSF under grants 2145631, 2215017, 2226447, 2326898, and the Defense Advanced Research Projects Agency (DARPA) under contract number D22AP00148.

References

[1] [n. d.]. Android IMSI-Catcher Detector. https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector.
[2] [n. d.]. USRP B210. https://www.ettus.com/all-products/ub210-kit/.
[3] 3GPP. 2024. *NR; Physical layer procedures for control.* Technical Specification (TS) 38.213. 3rd Generation Partnership Project (3GPP).
[4] 3GPP. 2024. *NR; Radio Resource Control (RRC); Protocol specification.* Technical Specification (TS) 38.331. 3rd Generation Partnership Project (3GPP).
[5] 3GPP. 2024. *Study on 5G security enhancements against False Base Stations (FBS).* Technical Report (TR) 33.809. 3rd Generation Partnership Project (3GPP).
[6] Lukas Arnold, Matthias Hollick, and Jiska Classen. 2024. 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*. 613–629.
[7] R. Barnes, S. Iyengar, N. Sullivan, and E. Rescorla. 2023. RFC 9345: Delegated Credentials for TLS and DTLS.
[8] Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz. 2021. 5G SUCI-Catchers: Still catching them all?. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 359–364.
[9] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. 2014. IMSI-catch me if you can: IMSI-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference*. 246–255.
[10] Yilu Dong, Rouzbeh Behnia, Attila A Yavuz, and Syed Rafiul Hussain. 2025. Securing 5G Bootstrapping: A Two-Layer IBS Authentication Protocol. *arXiv preprint arXiv:2502.04915* (2025).
[11] Mitziu Echeverria, Zeeshan Ahmed, Bincheng Wang, M Fareed Arif, Syed Rafiul Hussain, and Omar Chowdhury. 2021. Phoenix: Device-centric cellular network protocol monitoring using runtime verification. In *Network and Distributed System Security Symposium, NDSS*.
[12] Electronic Frontier Foundation (EFF). [n. d.]. Crocodile Hunter. https://github.com/EFForg/crocodilehunter
[13] Simon Erni, Martin Kotuliak, Patrick Leu, Marc Roeschlin, and Srdjan Capkun. 2022. AdaptOver: adaptive overshadowing attacks in cellular networks. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*. 743–755.
[14] Hui Gao, Yiming Zhang, Tao Wan, Jia Zhang, and Haixin Duan. 2021. On Evaluating Delegated Digital Signing of Broadcasting Messages in 5G. In *2021 IEEE Global Communications Conference (GLOBECOM)*. 1–7.
[15] Syed Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A systematic approach for adversarial testing of 4G LTE. In *Network and Distributed Systems Security (NDSS) Symposium 2018*.
[16] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino. 2019. 5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 669–684.
[17] Syed Rafiul Hussain, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino. 2019. Insecure connection bootstrapping in cellular networks: the root of all evil. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 1–11.
[18] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. 2019. Touching the untouchables: Dynamic security analysis of the LTE control plane. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1153–1168.
[19] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Čapkun. 2022. {LTrack}: Stealthy tracking of mobile phones in {LTE}. In *31st USENIX Security Symposium (USENIX Security 22)*. 1291–1306.
[20] Norbert Ludant and Guevara Noubir. 2021. SigUnder: A stealthy 5G low power attack and defenses. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 250–260.
[21] Kazi Samin Mubasshir, Imtiaz Karim, and Elisa Bertino. 2024. FBSDetector: Fake Base Station and Multi Step Attack Detection in Cellular Networks using Machine Learning. *arXiv preprint arXiv:2401.04958* (2024).
[22] Navid Nikaein, Mahesh K. Marina, Saravana Manickam, Alex Dawson, Raymond Knopp, and Christian Bonnet. 2014. OpenAirInterface: A Flexible Platform for 5G Research. *SIGCOMM Comput. Commun. Rev.* 44, 5 (oct 2014), 33–38.
[23] CheolJun Park, Sangwook Bae, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, and Yongdae Kim. 2022. {DoLTEst}: In-depth downlink negative testing framework for {LTE} devices. In *31st USENIX Security Symposium (USENIX Security 22)*. 1325–1342.
[24] M. Pease, R. Shostak, and L. Lamport. 1980. Reaching Agreement in the Presence of Faults. *J. ACM* 27, 2 (April 1980), 228–234.
[25] Syed Md Mukit Rashid, Tianwei Wu, Kai Tu, Abdullah Al Ishtiaq, Ridwanul Hasan Tanvir, Yilu Dong, Omar Chowdhury, and Syed Rafiul Hussain. 2024. State Machine Mutation-based Testing Framework for Wireless Communication Protocols. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*. 2102–2116.
[26] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2018. On the impact of rogue base stations in 4g/lte self organizing networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 75–86.
[27] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 221–231.
[28] Altaf Shaik, Jean-Pierre Seifert, Ravishankar Borgaonkar, N. Asokan, and Valtteri Niemi. 2016. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In *23rd Annual Network and Distributed System Security Symposium, NDSS, 2016*. The Internet Society.
[29] Ankush Singla, Rouzbeh Behnia, Syed Rafiul Hussain, Attila Yavuz, and Elisa Bertino. 2021. Look before you leap: Secure connection bootstrapping for 5g networks to defend against fake base-stations. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*. 501–515.
[30] SRLabs. [n. d.]. Snoopsnitch - Mobile Network Security Tool. https://github.com/srlabs/snoopsnitch.
[31] Kai Tu, Abdullah Al Ishtiaq, Syed Md Mukit Rashid, Yilu Dong, Weixuan Wang, Tianwei Wu, and Syed Rafiul Hussain. 2024. Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association.
[32] Simeon Wuthier, Jinoh Kim, Jonghyun Kim, and Sang-Yoon Chang. 2024. Fake base station detection and blacklisting. In *2024 33rd International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 1–9.
[33] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. 2019. Hiding in plain signal: Physical signal overshadowing attack on {LTE}. In *28th USENIX Security Symposium (USENIX Security 19)*. 55–72.