Fake Base Station Detection and Blacklisting

Sourav Purification*, Simeon Wuthier*, Jinoh Kim†, Jonghyun Kim‡, and Sang-Yoon Chang*
*University of Colorado Colorado Springs, Colorado Springs, CO, 80918, USA
Email: {spurific, swuthier, schang2}@uccs.edu
†Texas A&M University-Commerce, Commerce, TX, 75428, USA
Email: Jinoh.Kim@tamuc.edu
‡Electronics and Telecommunications Research Institute, Daejeon, 34129, South Korea
Email: jhk@etri.re.kr

***Abstract*—A fake base station is a well-known security issue in mobile networking. The fake base station exploits the vulnerability in the broadcasting message announcing the base station's presence, which is called SIB1 in telecommunications protocols such as 4G LTE and 5G NR, to get the user equipment to connect to itself. Once connected, the fake base station can deprive the user of connectivity and access to the Internet/cloud. We discover that a fake base station (which engages the user equipment until parts of the connectivity setup and then discontinues with the protocol) can disable the victim user equipment's connectivity for an indefinitely long time, which we validate using our threat prototype against current 4G/5G practice. We design and build a detection and blacklisting identification of the fake base station so that the user equipment can avoid the base station and move on to connecting to a legitimate base station for the connectivity availability. Our detection and blacklisting scheme builds on the standardized 5G protocol and requires the implementation only on the user equipment (no further protocol changes), facilitating practicality. Our scheme uses the real-time information of both the time duration and the number of request transmissions, which features are directly impacted by the fake base station's threat and have not been studied in the previous research. We implement both the base station and the user defense on software-defined radio using open-source 5G software (srsRAN and Open5GS) for validations. We vary the base station implementation to simulate legitimate vs. faulty-but-legitimate vs. fake-and-malicious base stations, where the faulty base station notifies the connectivity disruption and releases the session while the fake base station continues to hold the session. We empirically analyze the detection and identification thresholds, which vary with the fake base station's power and the channel condition. By strategically selecting the threshold parameters, our scheme provides zero errors, including zero false positives to avoid blacklisting the temporarily faulty base stations which can not provide the connectivity at the time.**

***Index Terms*—Telecommunications Networking, 5G, 6G, Fake Base Station, Detection, Blacklisting, Security, Availability**

I. Introduction

User equipment connects to the remote Internet and services through multiple nodes, the first of which is the base station. To support the mobility of the user equipment, it connects to the base station which serves as the bridge gateway between wireless vs. wired connection to the switches; the base station communicates to the user equipment in wireless communication and to the routers and servers in wired communications. The wirelessly connected user equipment thus requires the base station as the first hop (i.e., last-mile hop) in its communication path to the remote server and Internet. In telecommunications networking protocol, e.g., 4G, 5G, the base station sets up the wireless communication channel via the radio resource control (RRC), which includes the system information block (SIB) broadcasting communication to announce the base station's presence and delivery the communication-channel control information.

Malicious or fake base station is a well-known security issue in mobile networking. For example, there are open-source tools and tutorials for setting up fake base stations, e.g., [4], [9]. The fake base station exploits the vulnerability in the broadcasting SIB and RRC. Previous research launched the fake base station to manipulate the RRC and SIB communications to downgrade the security protection, misdirect the user equipment connection, and transmit fake public warning system messages, among others, as described in Section II. In contrast to the previous research, we focus on the fake base station's threat on the user equipment availability. The fake base station prevents the user equipment from connecting to a legitimate base station and therefore deprives it of its connectivity availability. We first investigate the fake base station and discover that a base station timing the disconnection start among the steps in the connectivity setup process can have much more availability damage; more specifically, the fake base station will complete the RRC setup but stop after receiving the first digital communication meant for the backend core network to continue to get the user equipment engaged and wasting its connection time and effort.

To defend against the fake base station, we design and build a detection and blacklisting identification scheme that requires the implementation or changes only at the user equipment, i.e., does not require any protocol-level changes or changes at any other entities beyond the base station. Once a fake base station gets detected and identified, the user equipment connects to a legitimate base station. We specifically design our scheme so that the detection and blacklisting minimize the false positives so that we avoid blacklisting a legitimate base station being faulty or having a temporary connection issue. Our scheme and its detection threshold control thus depend on the base-station-user-equipment channel condition and the fake base station's transmission power. Our scheme also makes use of the real-time observations directly related to the availability impact of the user equipment. Because the fake base station aims to have the user equipment connected and engaged to itself as long as possible, we use the time duration of the connectivity set up as well as the number of repeated request transmissions to inform and drive our scheme.

We implement our scheme using software-defined radio and

open-source 5G srsRAN software to validate our design. We implement and simulate the user equipment (implementing the defense) and the base stations, including legitimate and working well vs. faulty and temporarily-cannot-connect vs. fake and malicious base stations. Because of the lasting impacts of blacklisting, we simulate and analyze the faulty-but-legitimate base station which temporarily cannot provide connectivity; our scheme does not blacklist such base station.

The rest of the paper is organized as follows. Section II discusses the related works that focus on attacks and defenses against fake base stations exploiting radio and wireless communications. We provide relevant background information on overall 5G architecture with underlying protocols in Section III. We described our threat model with a clear distinction between fake base station and faulty base station in Section IV. In Section V, we explain our detection and blacklisting scheme, while Section VI provides a performance analysis of our scheme's experimental results using binary classification for detection and blacklisting. We discuss future directions in Section VII and conclude our paper in Section VIII.

II. Related Work

Fake base station assumes the base station functionality, including the wireless-communication capability and its role as a bridge gateway between wireless vs. wired networking. Therefore, its threats focus on the RRC and SIB communications, distinguishing the fake base station from other threat actors using injections. In this section, we thus focus on the fake base station threats on RRC and SIB, as opposed to generic digital communication injections. While much of these works focus on the threat mechanisms and impacts, our work focuses on the defense based on detection and identification to avoid the fake base station and connect to a legitimate base station for availability.

1) Threats on SIB and RRC: An attacker exploits the cell selection/reselection process (selecting the highest signal power [3]) and cryptographically insecure (without integrity and authentication protection) broadcast system information messages in radio control communication to launch a fake base station attack in LTE [13], [23] and even in 5G-NR [5], [6]. Lee et al [13] and Bitsikas et. al [6] demonstrate that the attacker can craft system information messages (e.g. MIB, SIB1) to set up RRC connection with the user equipment and dispatch false public warning messages after the setup. Moreover, the adversary also has the capability to trigger the handover process by modifying the cell reselection-related information in the system information messages [5]. In such attacks, the prerequisites are transmitting the signal at a higher strength than the legitimate base station [23] hence the base station with higher signal strength is always able to lure the user equipment to get connected to it.

Previous research also specifically studied the threat impacts after the fake base station makes the connection. Once the benign user equipment connects to the fake base station at the RRC layer, the adversary can launch protocol downgrade from 5G/4G to 2G (i.e. bidding down) attack [12], user equipment device identification attacks [17], launch SMS phishing attack [14], [22] and drain user equipment battery [10], [17]. Furthermore, as a secondary impact, the fake base station can disrupt user equipment connectivity to the legitimate base station by denial-of-service attacks and control the connection availability [10], [16], [18].

2) Defense Against Fake Base Station: While the previous research largely focused on the offensive side of the fake base station, more limited research detected and identified fake base stations using RF fingerprinting in wireless signal processing [25] and using the digital spam messages transmitted by the fake base station [14], [24]. These previous research are highly relevant to our work because they have the same goal of detecting and identifying fake base stations. However, our work uses the user equipment behavior as a result of connecting to the fake base station for the detection and identification and focuses on the RRC control communication to set up the connectivity. Our work focuses on the RRC control communication standardized by 3GPP [2], because the control communication is unique to the cellular base station. Our work is orthogonal to these previous detection/identification works and can be used in conjunction with them to provide a richer detection/identification; we focus on our novel contributions and the detection features of time and number of registration request packets in RRC in this paper.

Other research works [11], [15], [19] proposed the digital signature-based authentication of system information messages by legitimate base stations to prevent the user equipment from getting connected to the fake base station. Our defense work is distinguishable from these previous research works in the following ways. First, these previous works are preventive measures to disable the user equipment to connect to the fake base station; in contrast, our works detect and identify after the threat occurs. Second, these previous works involve greater systematic changes involving the protocol and algorithmic changes in the user equipment, base station, and the backend core network; for example, 3GPP is in the initial stages of conceptualizing and identifying the requirements of establishing the public key of the base station to enable such cryptographic approach [1]. In contrast, our work only requires the implementation on the user equipment, which is also the beneficiary of the scheme, and thus requires substantially fewer changes in the system implementation and standardization, facilitating practicality and deployability. Our work is therefore orthogonal to these previous works and can used in conjunction with the previous cryptographic approaches.

In cellular 4G/5G protocol, a limited number of research implemented security on the cellular base station against potentially malicious user equipment, e.g., for authentication [7], [8]. While the backend core network has traditionally authenticated the user equipment and established security, e.g., 5G authentication and key management (AKA), such an approach implementing security on the base station on the network edge can enable quicker mitigation and reduced threat impacts. Our work however considers the malicious base station (i.e., the threat actor is the base station), in contrast to these previous research defending against the malicious user equipment.

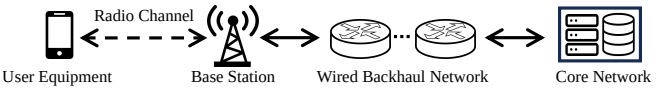


Fig. 1: Mobile network entities, including user equipment, base station and 5G core network

III. Background and Primer

In this section, we provide a brief overview of the telecommunication architecture and the connectivity setup process. In section III-A, we provide an overview of 5G network architecture as shown in Figure 1. We describe the wireless communication channel setup of radio resource control (RRC) between the user equipment to the base station in section III-B and the digital non-access stratum (NAS) between the user equipment and core network via a base station in section III-C. We borrow the RRC and NAS terms from the 3GPP 5G New Radio standardization and use it in our paper and show the protocol in Figure 2a; RRC is shaded in yellow while NAS is shaded in blue. Both the RRC-layer and NAS-layer protocol and interactions are for connectivity setup, i.e., once the NAS completes, the user equipment can use the connectivity service for remote access.

Our scheme design and implementation are based on the standardized 5G protocol. Although our detection and identification can apply to the earlier generations of telecommunication protocols, e.g., 2G-4G, we focus on the most recent 5G NR protocol because 5G is the most recent and has the strongest security in authentication and key agreement (AKA).

A. 5G Cellular Network Architecture

The 5G cellular telecommunication network has three main components: user equipment, base station, and core network. Figure 1 shows the physical connection diagram of these three components. The user equipment consists of a mobile device equipped with a universal subscriber identity module (USIM) that contains the subscriber-specific identity and network access-related identities (network ID, network public key, service type, etc.). The base station acts as a bridge gateway between the user equipment and the core network. The core network provides service connectivity to the user equipment by authentication management, identity management, and mobility management. The user equipment accesses the cellular network using a radio channel with the base station and establishes a logical connection with the core network over the established radio connection to get the cellular service. In the 5G cellular networking protocol, the user equipment connects to the base station using a radio resource control (RRC) layer connection and to the core network using a non-access stratum (NAS) layer connection. An intermediary wired backhaul network of routers and switches connects the base station and core network which is out of this research scope.

B. Radio Resource Control (RRC) for Wireless Communication Channel Control and Setup

Because user equipment connects wirelessly to the base station, RRC establishes the radio resource and the wireless channel, including the medium access control (MAC), between the user equipment and the base station.

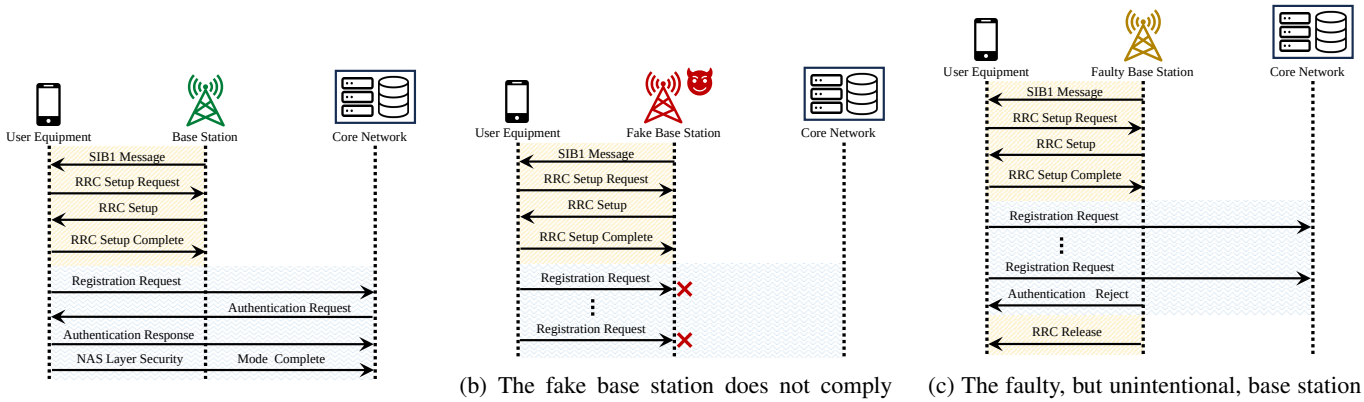
The user equipment deterministically selects a base station that has system information messages with the highest received signal power to establish the RRC layer connection using a three-way handshake. As illustrated in Figure 2a (yellow shaded), the RRC connection process begins with the base station periodically broadcasting system information messages with a specific downlink frequency. The system information messages consist of the Master Information Block (MIB) and System Information block messages. Among these messages, the System Information Block 1 (SIB1) is important for the user equipment to get network parameters for initiating the RRC connection with the base station. The System Information Block 1 (SIB1) contains network access-related information such as network identities (PLMN ID, cell ID), cell selection criteria such as minimum received signal strength/quality, and downlink/uplink frequencies. The PLMN ID is the unique identifier of the cellular network provider and the cell ID is the unique identifier of the base station broadcasting the SIB1. Before further proceeding with the SIB1, the user equipment selects the cell of the base station if the cell selection criteria are satisfied.

When there are multiple base stations nearby, the user equipment chooses the base station whose signal power for transmitting SIB1 is the greatest. After a user equipment is powered on, it scans for all radio frequencies in 5G New Radio (NR) bands and measures the received signal power (reference signal received power/RSRP and reference signal received quality/RSRQ). The user equipment attempts to select the cell of the base station to initiate a radio connection if both the received signal strength and received signal quality are greater than the minimum requirement specified in the SIB1 of the cell.

After radio signal-based base station/cell selection based on SIB1, as shown in Figure 2a, the user equipment proceeds to set up the RRC connection with the base station by sending the RRC setup request. Upon receiving the RRC setup request the base station accepts the connection request and sends the RRC setup message to the user equipment. The user equipment completes the RRC connection by sending the RRC setup complete message along with the Registration Request to initiate a NAS layer connection with the core network. This initial Registration Request is the first message for 5G authentication and key agreement protocol (5G-AKA). Section III-C discusses the 5G-AKA and NAS layer connection setup in detail.

C. Digital 5G-AKA and Non-Access Stratum (NAS) Setup

In 5G, the user equipment establishes the NAS layer connection with the core network after mutual authentication and key agreement (known as 5G-AKA) between them as shown in Fig. 2a (blue shaded) that uses public key cryptography. 4G does conduct AKA between the user equipment and core network, similar to 5G, but uses symmetric cryptography, unlike 5G. 5G therefore provides stronger security than 4G. The earlier generations before 4G, i.e., 2G and 3G, do not



(a) The legitimate base station operates according to 3GPP standardized protocol [2].

(b) The fake base station does not comply with the protocol and ceases transmission after receiving the Registration Request.

(c) The faulty, but unintentional, base station sends RRC Release and Authentication Reject notifying the connectivity disruption.

Fig. 2: The protocol between user equipment, base station, and core network for setting up the connectivity, including RRC and NAS. The RRC process between the user equipment and the base station (yellow-shaded) precedes the NAS process between the user equipment and the core network via the base station (blue-shaded). In NAS, the Registration Request can be repeated until the Authentication Request. The three figures differ in the base station nature scenarios: legitimate and working (green) vs. fake (red) vs. faulty (yellow).

implement or support AKA. In 5G-AKA, the user equipment encrypts its subscriber identity using the core network public key that is installed into its USIM card and sends it to the core network in the Registration Request message. After receiving the registration request from the user equipment, the core network verifies the user equipment subscriber identity using its private key and sends an authentication request to the user equipment with authentication parameters. The user equipment authenticates the core network using the authentication parameters and sends an authentication response (success or reject) to the core network. After mutual authentication between the user equipment and the core network, they negotiate ciphering and integrity protection algorithms for subsequent communication using the security mode procedure. After this procedure, both RRC and NAS layer connections use ciphering and integrity-protected algorithms.

5G and 4G AKA builds some resistance against fake base stations. More specifically, even if the fake base station can get the victim user to connect initially, the user can attempt to connect to the backend core network. In 5G AKA, the core network sends a digitally signed message after RRC as a part of the mutual authentication between the core network and the user (including the subscription verification of the user). Once receiving the digitally signed message, the user can verify the digital signature to authenticate the connection. However, such defense consumes the processing and energy resources of the mobile user disproportionately large so that the threat impact and the resource consumption (the digital communications after RRC and radio medium access control (MAC) and communicating to the backend which is multiple hops away) is significantly larger and disproportional to the attacker effort (SIB1 injection at RRC).

IV. Fake Base Station Threat

A. Threat Model

An attacker has the knowledge of the cellular 5G networking protocol by Kerckhoff's Principle and can launch a fake base station using software-defined radios and can exploit radio communication between the user equipment and the legitimate base station, e.g., there are even development tools and tutorials for setting up such fake base station,e.g., [4], [9]. The attacker exploits the deterministic base station selection procedure and the lack of integrity protection of system information messages, as described in Section III-B, to launch a fake base station attack. In our threat model, we consider such an attacker with a fake base station who can broadcast fabricated system information messages with higher signal power so that benign user equipment selects the cell of the fake base station over a legitimate base station that meets cell selection criteria. The adversary can adaptively choose signal transmission power gain to take control of the radio channel between the base station and the user equipment. Afterward, the fake base station can establish a radio resource control (RRC) connection with the user equipment and drop, modify, or inject upper-layer communication (e.g. NAS layer) from the user equipment to core the network later on.

B. Fake Base Station Threat Against Availability

In our work, the attacker has the goal of depriving and disabling the connectivity availability of the user equipment. As described in Section III-C, 5G AKA provides some resistance against the fake base station. The core network authentication verification using the USIM equipped within the user-equipment device can serve and indicate the legitimacy of the base station; the base station legitimacy check fails if the authentication fails.

Our threat occurs before the NAS and before AKA. In our threat, the fake base station injects the fake SIB1 message

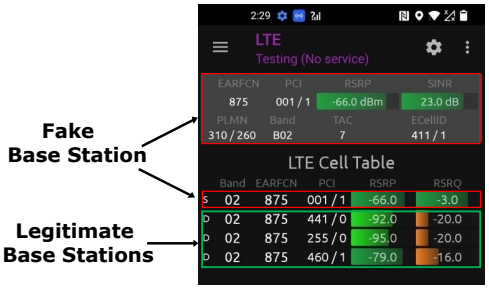


Fig. 3: Proof-of-concept fake base station attack on an Android user equipment connected to a real-world 4G LTE network.

to establish the RRC and wireless communication channel with the user equipment. The fake base station increases the transmission signal power to transmit the SIB1 with the highest signal power on the user equipment, which will have the user equipment connect to the fake base station as described in Section III-B. The fake base station continues with the RRC setup as depicted in the yellow-shaded region in Figure 2a. Once the RRC setup is complete, when the user equipment continues with the NAS-layer process and sends the Registration Request, the fake base station withholds sending it to the core network and stops the rest of the process. The fake base station does not comply with the protocol and ceases transmitting any transmissions following/after receiving the user equipment's Registration Request, as described in Figure 2b. In Figure 3, we show a proof-of-concept fake base station attack on an Android user equipment connected to a real-world 4G LTE using our threat prototype described in Section VI. The fake base station establishes the RRC connection by sending system information messages with higher signal strength and it maintains the connection with the user equipment as long as it wants. As a consequence, the user equipment gets deprived of cellular services from the legitimate base stations.

The timing of the fake base station threat stopping the connectivity setup RRC/NAS process is critical for the availability impact. If the fake base station stops the RRC/NAS before the Registration Request, then the user equipment gets disconnected as soon as the process stops. Also, the fake base station cannot proceed with the Authentication Request because it does not hold the core network's private key (or, if 4G, the symmetric key) and cannot generate the correct digital signature; the user equipment can check the legitimacy of the core network/base station and disconnects the NAS/RRC immediately. However, the user equipment is persistent with the Registration Request by 5G design because there can actually be accidental connectivity availability due to the failure in the base station and the further away core network.

C. Faulty But Legitimate Base Station

Our blacklisting identification focuses on the attacker (fake base station) and not on the accidental/unintentional failures (faulty base station). We therefore distinguish between fake vs. faulty-but-unintentional, the latter of which can be caused by the lack of connectivity services at the time of the user equipment access. The base station cannot provide connectivity at some times, which are often temporary, i.e., the faulty base station operates correctly at other times. The 3GPP 5G NR supports such temporary faulty cases not having connectivity, and our work builds on the protocol for such faulty cases. For accidental *faulty base station*, we continue with the NAS process for the connectivity setup but, if it fails, the base station sends a RRC Release message to the user equipment and the reject cause, e.g., Authentication Reject. The accidental faulty base station thus releases the RRC connection with the user equipment, while the adversarial fake base station continues to hold on to the RRC connection depriving its availability further. The faulty base station differs from the fake base station in that it explicitly releases and ends the connectivity setup. The faulty (and legitimate) base station operation is described in Figure 2c (in contrast, the legitimate and working-well base station operation is depicted in Figure 2a).

V. Our Detection and Identification Scheme

In our scheme, the user equipment adds a timer-counter-based detection and a blacklisting identification to defend against the fake base station threat described in Section IV. To make the detection/blacklisting decision, our scheme uses the sensing measures which are directly from the user equipment's availability experience impact resulting from the base station connectivity behavior. More specifically, our scheme uses the time duration for the connectivity setup (T) and the repeat transmissions count to set up the connectivity (N). Because our objective is to reduce the availability threat impact, we use T and N which are inherently impacted by the threat. Our scheme also implements the sensing and computing/logic only on the user equipment and does not require any additional changes in the protocol, facilitating the practicality and deployment of our scheme.

For detection, the user equipment tracks both the time duration starting from the initial Registration Request in the NAS layer (T) and the number of Registration Request transmissions it repeats (N). N is equal to one or is a small number when the user equipment connects to a legitimate base station, as the legitimate base station has the connectivity to the core network and can provide the connectivity, as shown in Figure 2a; in our experimentation which we will describe in Section VI, $N = 1$ without needing to send another Registration Request. In contrast, N is larger if the user equipment connects to a faulty base station and when there is no connectivity to the core network (Figure 2c), and N is infinite and unbounded if it connectes to a fake base station (Figure 2b). The Registration Request corresponds to the first transmission in the NAS in Figure 2a. If T exceeds τ_T **and** N exceeds τ_N, i.e., $T > \tau_T$ and $N > \tau_N$, then our scheme detects the fake base station. In our scheme, τ_T is the threshold for time duration (T) and τ_N is the threshold for the number of Registration Request (N). Because the Registration Request and the connectivity setup are specific to one base station identified by the Cell ID, the user equipment further blacklists the cell ID of the fake base station.

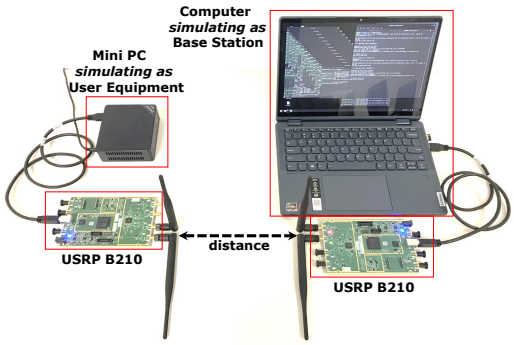


Fig. 4: Hardware setup for our implementation and experiment where the distance between the base station and user equipment is 5 meters. The backend core network coexists with the base station in the same computer.

We select the τ_T and τ_N to detect and identify the fake base station. We focus on identifying the fake base station as opposed to the accidental faulty base station, as described in Section IV-B, and therefore design our scheme to detect and identify the fake base station only. τ_T and τ_N increases as the communication channel between the user equipment and base station is worse, although the user equipment selects the base station with the greatest signal power strength as described in Section III-B. τ_T and τ_N, therefore, vary depending on the user equipment's observed channel state information[1].

VI. Implementation and Experimental Results

We simulate the base station (and the backend core network) using a computer and the user equipment using a MiniPC, both of which include USRP B210 software-defined radios for the radio front-end. We use *srsRAN* [20] for implementing the fake base station and the user equipment. To implement the backend 5G standalone core network, we use *Open5GS* [21]. We modify the NAS and RRC layer source codes in *srsRAN* at the base station and the user equipment to implement our attacks and defense mechanisms respectively. Figure 4 shows our hardware setup for the implementation and experimentation.

This section focuses on our experimental results with the faulty vs. fake base stations. We verify that the connection works well with the legitimate base station (demonstrating the correctness of the 5G implementation) and that the fake base station can deprive the user equipment for an indefinite time. The faulty base station experiment in Section VI-C informs the τ_T and τ_N selections. We vary and analyze the τ_T and τ_N parameters of our scheme for detecting and blacklisting the fake base station in Section VI-E; we also experimentally show how the use of both T and N measurements outperforms using either in our scheme.

A. Implementation and Experimental Setup and Optimality for Threshold Selection

Legitimate vs. Faulty vs. Fake Base Stations We implement the base station and the user equipment along with the connectivity setup between them described in Section III-B, including RRC and NAS. We conduct three experimental scenarios where the base station is legitimate vs. faulty vs. fake. The legitimate base station operation is described in Section III-B, while the faulty (accidental) and fake operations are described in Section IV-C and IV-B respectively. The faculty, but legitimate, base station ends the connectivity setup of NAS via Connection Release; in contrast, the fake base station continues to hold on to the NAS communication without explicitly ending the RRC/NAS connectivity setup.

Our Scheme Variants Using Different Observations Our scheme uses both the time duration T (the detector threshold is τ_T) and the number of Registration Requests N (the detector threshold is τ_N) as described in Section V. In this section, we compare our scheme with *our scheme variants* of using T only and using N only to better motivate the use of both T and N. Our scheme using both T and N for the detection and blacklisting outperforms the variants using T only or using N only.

Optimality for Threshold Selection We define *optimality* with respect to the error performance. More specifically, we achieve optimal accuracy performance if the false-positive error is minimized and then the false-negative error is minimized. If we can achieve zero false-positive rate, we then minimize the false negative rate. The false-positive error is prioritized because we design blacklisting and prioritize avoiding blacklisting legitimate base station which can be faculty (accidentally can not provide connectivity at the time). The thresholds achieving optimality does not need to be unique, i.e., there can be multiple thresholds which achieve minimum error performances. In fact, in our experiment, we have multiple thresholds achieving zero error (zero false-positives and zero false-negatives) and we choose the lowest threshold values to make the detection more sensitive.

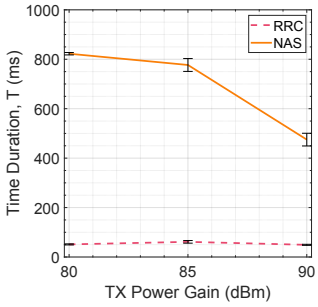
B. Testing Without Our Scheme: No Availability Against Fake Base Station

We empirically validate that the 5G connection works well when the base station is the legitimate base station. Against a fake base station, we implement enabling vs. disabling our scheme. This section focuses on the case when our scheme is disabled, while Section VI-E analyzes when our scheme is enabled against fake base stations (as well as legitimate and faulty base stations). The fake base station when our scheme is disabled can engage and hold the user equipment as much as it wishes. We implement the duration control for such withholding, and the user equipment attempts to connect to the fake base station by transmitting the Registration Request packets until the fake base station responds. If the fake base station chooses to continue to withhold, the user equipment continues with the connectivity setup protocol without trying another base station, depriving of its connectivity availability.

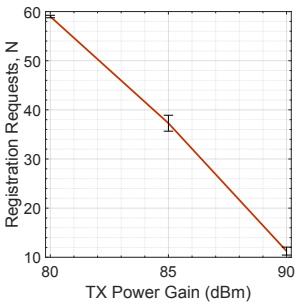
C. Faulty (But Legitimate) Base Station Experiment

We validate the RRC and NAS layer setup measurements from faulty (but legitimate) base station experiments while varying the base station transmission power gain as shown in

[1]Channel state information or CSI is commonly used in modern communication signal processing, for example, MIMO.



(a) RRC and NAS time duration between the UE and base station



(b) Number of registration requests sent by the user equipment

Fig. 5: Faulty but legitimate base station experimentation measurements at the user equipment while varying transmission power at the base station. The plots include the averages and the 95% confidence interval.

Figure 5. We select three different transmission powers (80 dBm, 85 dBm, and 90 dBm) of the base station to simulate the different channel conditions between the user equipment and the base station to measure the impact of received signal power on RRC setup and NAS setup for the worst case of a faulty but legitimate base station. In this experiment, the user equipment connects to the base station only when the base station transmission power is greater or equal to 80 dBm.

Figure 5a shows the RRC setup and NAS setup time duration when varying base station signal transmit power. The RRC setup time stays relatively consistent and only varies from 49 ms-61 ms for three different transmission power gains of the base station. However, the NAS setup time duration decreases as the signal power gain increases which indicates that the NAS connection setup time depends on the received signal power at the user equipment i.e. radio channel conditions. As compared to the RRC setup time, the NAS setup connection time at 80 dBm power level is 822.42 ms while 474.94 ms at the highest power gain. Hence, within this time duration, the user equipment keeps sending Registration Requests to the core network until it gets an RRC release message from the faulty base station as discussed in Section IV-C.

We also validate the number of Registration Requests sent by the user equipment during NAS setup in the experimentation while varying the base station transmission power as illustrated in Figure 5b. The figure shows the number of Registration Requests also depends on base station transmission power i.e. received signal power at the user equipment. The number of requests is 60 at the lowest transmission power whereas it is 11 at the highest signal power. We also observe that the user equipment sends the Registration Request with an interval of 11 ms approximately.

D. Faulty Experiment Informs Threshold Control

We use fake base station detection and blacklisting while ensuring that faulty base stations are not detected as fake base stations and blacklisted. Blacklisting a temporarily faulty base station, e.g., no connectivity at the time, can have a lasting impact on the base station and deprive the user equipment of options when trying to access the cellular service in the future. Because of this importance, our analyses focus on the false positive probability/rate, corresponding to when the base station is actually legitimate but faulty but our scheme detects it as a fake base station and blacklists it. The concrete analyses for our detection threshold control is described in the next section, Section VI-E.

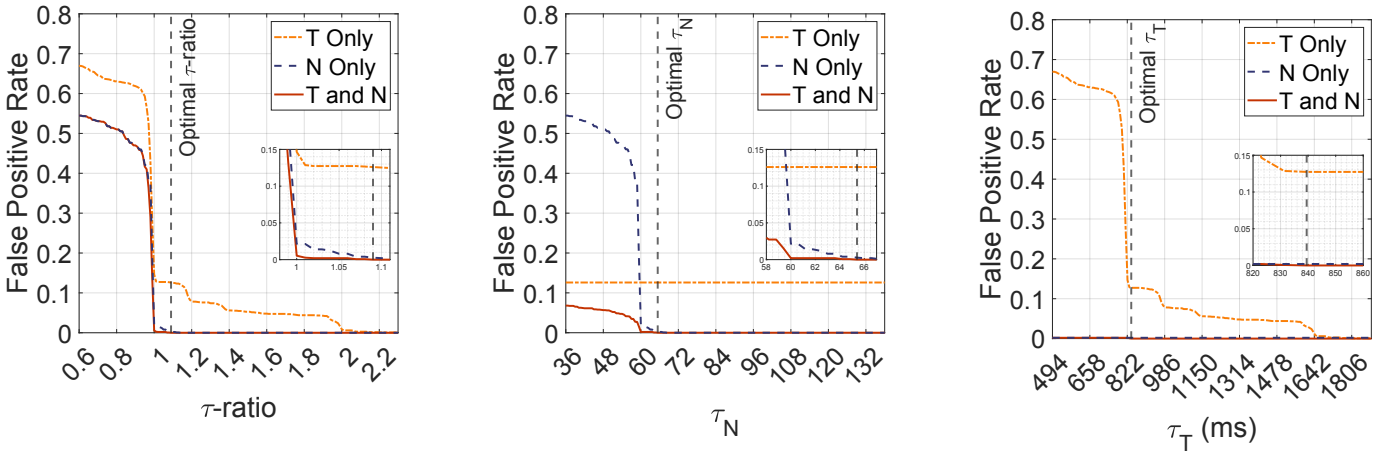
E. Detection Accuracy Performance Against Fake Base Station

We test our scheme against a legitimate base station, a faulty (but legitimate) base station, and a fake base station. While varying τ_T (494ms $< \tau_T <$ 1893ms) and varying τ_N ($36 < \tau_N < 138$), our scheme correctly decides the legitimate base station and the fake base station with 100% accuracy, i.e., our scheme yields 0 (no fake base station) for all of the legitimate base station experiments and it yields 1 (yes base station) for all of the fake base station. Against a legitimate base station, our scheme correctly does not detect and blacklist the base station. Against fake base station persistently withholding the connection, our scheme correctly decides that it is a fake base station and the false negative rate is zero.

In the faulty (but legitimate) base station experiments, i.e., when testing our scheme against the faulty base station, we observe errors when varying τ_T and τ_N. Because the faulty base station is still legitimate, it is incorrect to detect, classify, and blacklist it as a fake base station. Varying τ can yield false positives where a faulty base station's connectivity setup (RRC/NAS) gets detected and blacklisted as a fake base station. We analyze such error because we want to reduce and avoid blacklisting a faulty and legitimate base station.

We vary the τ thresholds (τ_T and τ_N) and compare our scheme using both T and N observations vs. our scheme variant using only T vs. our scheme variant using only N. We first jointly vary τ_T and τ_N and show our results. To jointly vary the τs, we introduce *τ-ratio* which is the ratio between the τ value and some reference value τ_0. τ_T-ratio is equal to $\frac{\tau_T}{\tau_{T,0}}$ where $\tau_{T,0}$ = 823 ms; τ_N-ratio is equal to $\frac{\tau_N}{\tau_{N,0}}$ where $\tau_{N,0}$ = 60 requests. For example, if τ_N-ratio is equal to two, τ_T = 1646 ms which is doubled from $\tau_{T,0}$ = 823 ms. While the reference values (the denominators of the τ-ratio) can be chosen differently, we choose $\tau_{T,0}$ = 823 ms and $\tau_{N,0}$ = 60 requests, as these are the average values (rounded) of the faulty base station experiments when the base station's transmission power is the lowest and thus the values are the highest, which is describe in Section VI-C. In Section VI-C, we observe that the 95% confidence intervals is small so we expect $\tau_T = \tau_{T,0}$ = 823 ms and $\tau_N = \tau_{N,0}$ = 60 to have a relatively small number of false positive errors.

Figure 6a shows the results of the joint varying of τ_T and τ_N while fixing τ_T-ratio and τ_N-ratio to be equal, i.e., τ_T-ratio = τ_N-ratio. The false-positive rate/probability decreases as we increase τ for both T and N, because increasing τ reduces the detection sensitivity and the occurrences of detecting 1 (deciding that it is a fake base station). We also see that our scheme using both T and N observed information outperforms our scheme variants using either. For example, when τ_T-ratio and τ_N-ratio are both equal to one (i.e., τ_T = 823 ms and τ_N



(a) τ_T and τ_N vary jointly (b) $\tau_T = 897$ ms and τ_N varies (c) $\tau_N = 66$ and τ_T varies

Fig. 6: Error (false positive rate) performances while varying τ. Figure 6a jointly varies τ_T and τ_N with equal τ-ratio.

= 60), our scheme false positive rate is 0.0053, while using T only has the false positive rate of 0.1467 and using N only has the false positive rate of 0.0213. Using both information provides better/lower error rates. While our scheme using both T and N provides a very small false positive rate of 0.0053, it still provides errors and blacklists the faulty-but-legitimate base station with a probability of 0.0053.

Our thresholds selection is based on the optimality definition in Section VI-A, e.g., to minimize the error performance. Because we already achieved a zero false-negative rate, i.e., all the fake base station experimental samples are detected, our threshold selections achieve optimality by yielding a zero false-positive rate. In Figure 6a, the optimal τ-ratio is equal to 1.09 if τ_T-ratio = τ_N-ratio, i.e., τ_T is equal to 897 ms while the optimal τ_N is equal to 66.

Figure 6b and Figure 6c vary the two threshold parameters unilaterally without the constraint of τ_T-ratio = τ_N-ratio, i.e., we fix one threshold while varying the other. The fixed values are the optimal values in Figure 6a when we jointly varied the detection threshold parameters, i.e., $\tau_T = 897$ ms and $\tau_N = 66$. Figure 6b varies τ_N while fixing τ_T = 897 ms. Our scheme variant using T only has a constant error performance value because that scheme only uses T compared to $\tau_T = 897$ ms; N is not used and varying τ_N has no effect on this scheme variant. Because $\tau_T = 897$ ms, our scheme using both T and N provides better than jointly varying τ_T and τ_N when τ_N is less than $\tau_{N,0}$ = 60. Fixing $\tau_T = 897$ ms, the optimal τ_N is equal to 66.

When varying τ_T while fixing $\tau_N = 66$ in Figure 6c, the optimal τ_T is equal to 840 ms. This optimal τ_T is different and lower than 897, the optimal τ_T threshold value when jointly varying the detection thresholds with the constraint of having equal τ_T-ratio and τ_N-ratio in Figure 6a. Based on these results, our scheme uses $\tau_T = 897$ ms and $\tau_N = 66$ to provide zero errors in our experiment involving legitimate, faulty (but legitimate), and fake base stations.

VII. Future Directions Discussions

More Advanced Threats Similarly to many other detection-based schemes, there can be a fake base station to avoid detection, i.e., it does not get detected as a faulty base station, but that would result in the attacker reducing its availability threat impact and releasing the connectivity setup. This effectively reduces the fake base station behavior to the faulty base station behavior, i.e., the attacker behaves like a faulty base station. We consider our detection to be successful because, in such case, the attacker behavior reduces to a legitimate-but-faulty base station and it explicitly releases the connection. While our scheme does not raise the flag for detection/blacklisting, it effectively reduces the threat impact on availability.

There can also be a Sybil threat where the fake base station generates and changes its ID (cell ID) to evade detection and blacklisting. Recent advancements in the 3GPP standardization have initiated introducing public keys for base station [1], which can enable the prevention and defense against such Sybil threat. We can also explore a responsive defense scheme using the base station behaviors beyond just the received power strength or randomization on the base station selection.

An attacker can attempt to launch a threat beyond just availability and disrupting the connectivity, such as attempting the victim user equipment to connect to a fake server. However, due to the core network's public key in the user equipment's physical USIM as described in Section III-C, such threat requires breaking public-key cryptography (public-key key exchange) and is thus infeasible.

Advancing Detection Our work focuses on the threat detection and blacklisting focusing on the fake base station with malicious intent. Our work can extend to a multi-class detection scheme to have distinct layers and levels for different classes, including the anomaly of faulty. For example, instead of the binary classification of fake vs. legitimate, we can combine anomaly and threat detection and introduce three classes of fake vs. faulty vs. legitimate.

For a richer detection, we can combine our information features for detection and blacklisting with those from the

previous research described in Section II-2. However, we focus on our research/novelty contributions (the observations of the time and number of request transmissions, which have not been analyzed in the previous research in fake base station detection) and their performances and analyses in this paper.

Another future direction will be to design and implement dynamic and adaptive schemes. Such dynamic control and adaptability can apply for detection, including controlling and varying the threshold values.

Machine learning, for example, reinforcement learning based on connectivity service reward or anomaly detection based on the deviations from the set protocol, can be used as an alternative mechanism for detection.

Advancing Blacklisting and Active Control While our current work focuses on blacklisting, how such blacklisting is used for active control remains as future work. We expect our blacklisting to inform the base station selection, but the concrete mechanisms to address the how to inform and utilize the blacklisting remains as future work.

VIII. Conclusion

We design and build a fake base station detection and blacklisting identification scheme against fake base stations for the user equipment. We implement and validate different base station scenarios (legitimate, fake, and faulty) using software-defined radios and open-source software srsRAN. We empirically implement the faulty base station scenario and measure the time duration for RRC and NAS to evaluate the performance of our scheme. We analyze the performance of our scheme by varying the threshold values to get the optimal thresholds so that our scheme detects and blacklists only fake base stations instead of faulty but unintentional base stations i.e. zero false positives. We find that using both NAS layer connection time and the number of Registration Requests as thresholds rather than using either one of them provides better performance in terms of detecting fake base stations but not faulty base stations.

Acknowledgement

This work was supported by the National Science Foundation under Grant No. 1922410 (50%) and by the Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No.2021-0-00796, Research on Foundational Technologies for 6G Autonomous Security-by-Design to Guarantee Constant Quality of Security, 50%).

References

[1] 3GPP. TR 33.809 version 0.8.0 , "Study on 5G security enhancements against false base stations," 2021.

[2] 3GPP. TS 33.331 version 17.2.0 , "5G NR; Radio Resource Control (RRC); Protocol specification," 2022.

[3] 3GPP. TS 38.304 version 17.0.0, "5G-NR; User Equipment (UE) procedures in idle mode and in RRC Inactive state ," 2022.

[4] Adam M Toscher,Simone Margaritelli, "Awesome-Cellular-Hacking Public," https://github.com/W00t3k/Awesome-Cellular-Hacking, 2023, [Online; accessed 20-Feb-2024].

[5] E. Bitsikas and C. Pöpper, "Don't hand it over: Vulnerabilities in the handover procedure of cellular telecommunications," in *Annual Computer Security Applications Conference*, 2021, pp. 900–915.

[6] ——, "You have been warned: Abusing 5g's warning and emergency systems," in *Proceedings of the 38th Annual Computer Security Applications Conference*, 2022, pp. 561–575.

[7] Z. Cao, X. Zhou, M. Xu, Z. Chen, J. Hu, and L. Tang, "Enhancing base station security against dos attacks in wireless sensor networks," in *2006 International Conference on Wireless Communications, Networking and Mobile Computing*, 2006, pp. 1–4.

[8] S.-Y. Chang, A. Sarker, S. Wuthier, J. Kim, J. Kim, and X. Zhou, "Base station gateway to secure user channel access at the first hop edge," *Computer Networks*, vol. 240, p. 110165, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128623006102

[9] Hackers Arise, "Mobile or Cellular Hacking," https://www.hackers-arise.com/mobile-or-cellular-hacking, 2023, [Online; accessed 20-Feb-2024].

[10] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "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*, 2019, pp. 669–684.

[11] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "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*, 2019, pp. 1–11.

[12] B. Karakoc, N. Fürste, D. Rupprecht, and K. Kohls, "Never let me down again: Bidding-down attacks and mitigations in 5g and 4g," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, New York, NY, USA, 2023, p. 97–108.

[13] G. Lee, J. Lee, J. Lee, Y. Im, M. Hollingsworth, E. Wustrow, D. Grunwald, and S. Ha, "This is your president speaking: Spoofing alerts in 4g lte networks," in *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, 2019, pp. 404–416.

[14] 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." in *NDSS*, 2017.

[15] A. Lotto, V. Singh, B. Ramasubramanian, A. Brighente, M. Conti, and R. Poovendran, "Baron: Base-station authentication through core network for mobility management in 5g networks," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023, pp. 133–144.

[16] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "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*, 2018, pp. 75–86.

[17] ——, "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*, 2019, pp. 221–231.

[18] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," in *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*. The Internet Society, 2016.

[19] A. Singla, R. Behnia, S. R. Hussain, A. Yavuz, and E. Bertino, "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*, 2021, pp. 501–515.

[20] Software Radio Systems, "srsRAN Project," https://github.com/srsran/srsRAN_Project, 2022.

[21] Sukchan Lee, "Open5GS," https://github.com/open5gs, 2022.

[22] H. Wen, P. Porras, V. Yegneswaran, and Z. Lin, "Thwarting smartphone sms attacks at the radio interface layer," in *30th Annual Network and Distributed System Security Symposium, NDSS*, 2023.

[23] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on {LTE}," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 55–72.

[24] Y. Zhang, B. Liu, C. Lu, Z. Li, H. Duan, S. Hao, M. Liu, Y. Liu, D. Wang, and Q. Li, "Lies in the air: Characterizing fake-base-station spam ecosystem in china," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 521–534.

[25] 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.