Denial of Service Attacks Targeting Layer 2 in 5G RAN

Arpit Tripathi
IIT Hyderabad

Ashutosh Rajput
IIT Hyderabad

Ashit Kumar Subudhi
IIT Dharwad

Koteswararao Kondepu
IIT Dharwad

Abhishek Thakur
IDRBT Hyderabad

Bheemarjuna Reddy Tamma
IIT Hyderabad
tbr@iith.ac.in

2025 IEEE Future Networks World Forum (FNWF) | 979-8-3315-9193-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/FNWF66845.2025.11317524

***Abstract*—Denial of Service (DoS) attacks on legitimate users using a Fake Base Station (FBS) remain a persistent threat to the integrity and reliability of 5G networks. These attacks exploit gaps in lower-layer authentication procedure by impersonating legitimate base stations, resulting in wastage of radio resources. Traditionally, these attacks and their detection techniques often operate at the Non-Access Stratum (NAS) or Radio Resource Control (RRC) layers, missing the signs of such attacks originating at Layer 2. In this work, we introduce two DoS attacks on Random Access Channel (RACH) and RRC procedures over 5G RAN and study their impact on users. We further introduce a user-side threshold-based FBS detection technique to mitigate the impact of FBS. We demonstrate these DoS attacks and assess the effectiveness of the proposed detection technique on both physical testbed and simulation environments. Attack scenarios, including *RACH drop* and *RRCSetupRequest drop*, are emulated to demonstrate the effectiveness of these attacks. The results indicate that the proposed DoS attacks using FBS can significantly drain radio and compute resources, even without going through the registration process. With a threshold-based detection technique, we can minimize the impact of these attacks before they escalate.**

***Index Terms*—Fake Base stations, 5G, DoS attacks, Network Security, Radio Access Networks**

I. Introduction

With its diverse range of use cases, including massive Machine Type Communications (mMTC) and Ultra-Reliable Low-Latency Communications (URLLC), 5G is set to play a pivotal role in enabling a wide array of critical and real-time applications [1]. These applications span various industry verticals, including financial technology, transportation, healthcare, defense, and space exploration. As such, 5G and Beyond (5GB) networks are increasingly becoming an integral part of critical infrastructure that supports national and global services [2]. The rapid expansion of 5G networks has drawn increased attention from attackers, largely because of the vulnerabilities that have been highlighted in the previous research studies [3]. One notable attack scenario involves deployment of rogue base station or FBS [4], where a malicious FBS spoofs the cell identifiers like Public Land Mobile Network Identifier (`PLMN ID`), Physical Cell Identifier (`PCI`), and Tracking Area Code (`TAC`) of a legitimate base station (LBS) and engages legitimate UE in a fake registration procedure.

UE while changing its geographical location, follows a handover procedure that switches among various RRC states: `RRC_IDLE`, `RRC_INACTIVE`, and `RRC_CONNECTED`. More details about the handover procedure can be referred from the 3GPP specs on 5G NR [5]. The handover could be either network driven or UE driven [6]. UE, while attempting a handover procedure, may lose connectivity to the network due to radio link failure [6]. The registration procedure in the event of radio link failure is UE driven. This means that the UE will scan for the broadcast messages coming from the neighboring cells and select the cell with the best signal quality parameters like `RSRP/RSRQ` [5]. FBS can utilize this situation and may broadcast the parameters with a higher signal strength and force legitimate UEs to camp with its cell. The UE is then engaged in an unsuccessful registration loop with that FBS and thereby leading to DoS attack. We address these attacks as FBS attacks in the paper. As per the 3GPP specs, the UE blacklists such cells for a pre-defined duration - `T320` timer [5] before attempting to re-register with other nearby cells. However, the UE may attempt re-registration with the same cell after the `T320` timer expires. Neither the operator nor the fellow UEs are aware of this blacklisting procedure carried out by the individual UE. Effectively identifying or mitigating FBS attacks at the UE side is crucial to avoid major service disruptions [7] for other UEs and the mobile network operators.

Several prior works have tried addressing FBS attacks. Most of these works focused on signaling anomalies at NAS/RRC layers. For example, works by Mubasshir et al. [8] and Kriaa et al. [9] presented multi-step attacks using signal strength. The authors further utilized machine learning and knowledge graph inference techniques to identify suspicious behavior. Similarly, Wen et al. [10] presented attacks at the time of handover in case of RRC mechanism. They introduced O-RAN compliant L3 detection service utilizing xApp for radio resource management events and network signaling patterns. These techniques provide valuable insights to detect FBS, they tackle issues only when the attack has propagated to the upper layers, limiting timeliness and responsiveness. These techniques depend heavily on centralized data aggregation which may cause scalability issues and real-time effectiveness. Another set of studies by Saedi et al. [11] and Huang et al. [12] utilize deep learning and SDR platforms to extract L1 features for FBS detection using O-RAN architecture. These

Authorized licensed use limited to: Parul Institute of Engineering and Technology. Downloaded on September 15,2026 at 17:47:27 UTC from IEEE Xplore. Restrictions apply.

xApps use AI to characterize base stations but face a significant challenge of retraining and potential delays that may arise due to centralized data collection mechanism. Network-driven FBS detection mechanism like Murat [4] use position discrepancies to detect FBS. This technique avoids dependency on UEs, but lack real-time detection capabilities. Similarly, large-scale simulations like [13] explain signal strength attack scenarios and detection, but lack information on real-time or commercial grade devices. There are works that have focused on lower layers. Ludant et al. [14] presented vulnerabilities in lower layer control procedures. These emphasize risks from unprotected MAC layer. These techniques face deployment barriers due to protocol changes and concerns about backward compatibility.

In contrast to previous contributions, our work targets the FBS attacks on layer 2 of 5G RAN. The layer 2, in the event of failure, escalates the decision making to the upper layers for further analysis and evaluation [5]. For example, the decision to abort or retry a `RRC Connection Resume` may be triggered by the NAS layer. Our FBS attacks, which exploit lower-layer procedures such as `RACH` and `RRCSetup`, can therefore escalate these initial failures to the upper layers, where the decision to abort or retry are ultimately made. To the best of our knowledge, previous works presented FBS attacks that occur during the device registration phase at NAS and beyond, but paid little or no attention to attacks that arise at layer 2 - during the RACH procedure or the RRC Setup phase. The key contributions of this work are as follows:

- Introducing FBS attacks at Layer 2 and experimentally demonstrating their impact on the users.
- Proposing a threshold-based detection technique that allows the UE to detect DoS attacks targeting layer 2.

The rest of the paper is organized as follows. Section II presents the system model including the adversary model. Section III gives a brief overview of the detection technique. The experimental setup along with data collection step is explained in Section IV. Section V presents the result followed by discussion. Finally, Section VI presents the concluding remarks.

II. System Model

This section presents the system assumptions relevant to the work and the types of base stations relevant for our study.

A. System Assumptions

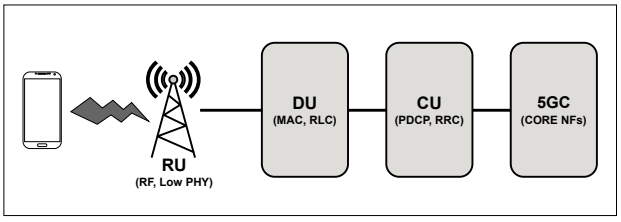


Fig. 1: System Model

We consider a 5G RAN deployment featuring a disaggregated RAN composed of CU, DU, and RU. Normally, a sufficient number of RUs is deployed to ensure overlapping coverage with adequate signal strength throughout the geographic area. UEs are mobile and attach to the strongest cell in the area, as determined by measurements such as `RSRP/RSRQ`. The mobility of UEs requires the use of handover mechanisms specified in 3GPP specs [5]. The `RACH` procedure and its related failures are explained below:

1) RACH Procedure: The `RACH` procedure establishes uplink synchronization between the UE and the base station (gNodeB) as seen in Fig. 2. The UE selects a random access (RA) preamble from a predefined list and transmits it to the network as `Msg1` over the physical random access channel (PRACH). The gNodeB responds with `Msg2`, which includes timing advance, an initial uplink grant, and the random access preamble identifier. Using this uplink grant, the UE sends `Msg3` containing the RRC setup request to initiate connection establishment. The gNodeB processes `Msg3` and returns `Msg4`, the contention resolution message. Through this process, the UE is assigned a Cell Radio Network temporary identifier (C-RNTI).

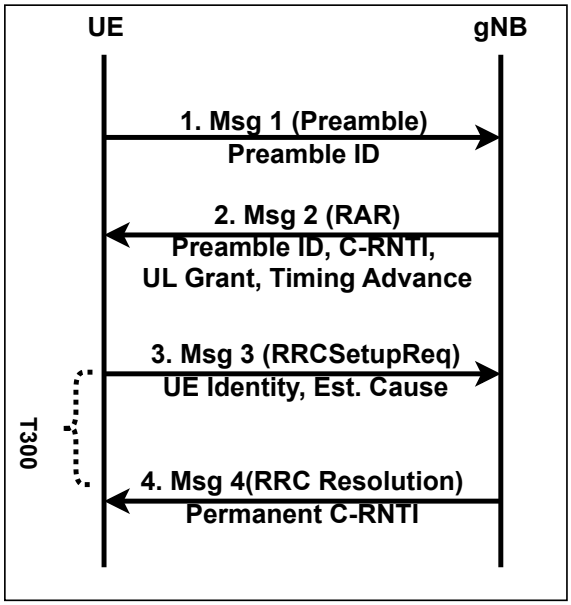


Fig. 2: Standard RACH Procedure

2) RACH Failures: In the event of `RACH` failure, the UE waits for the predefined `ra-ResponseWindow` before retrying the initial `RACH`. The maximum number of retries is determined by the `preambleTransMax` parameter, configured by the mobile operator and advertised to the UEs in `SIB1` messages transmitted by gNodeB [5]. Since the operator sets this parameter, the UE only becomes aware of it only after initiating the `initial attach` procedure. Likewise,

Authorized licensed use limited to: Parul Institute of Engineering and Technology. Downloaded on September 15,2026 at 17:47:27 UTC from IEEE Xplore. Restrictions apply.

after transmitting Msg3, the UE starts timer T300 to await a response. If the response (Msg4) is not received from the gNodeB within this period, the UE reports a connection establishment failure and retries the entire RACH procedure as explained in the previous section. The allowed number of such retries is also specified in the SIB1 configuration [5]. After the retries in both cases, it is noted that the UE abandons the cell selection process for a defined period before re-attempting RACH procedure. However, it is up to the upper layers on the UE side to take further decisions on connection re-establishment.

B. Types of Base Stations

To further add to the system model, we categorize base stations as follows: a) Legitimate (LBS) and b) Fake (FBS). The mobile operator deploys the LBS and strictly conforms to the relevant 3GPP specs. It authenticates users and correctly transmits network information. LBS may experience benign fluctuations but always responds to recovery procedures. LBS serves as the ground truth for normal network behavior and can therefore be used to identify anomalous activity by FBS.

The FBS represents an adversary in the 5G network deployed by the operator. These are deliberately deployed to impersonate legitimate base stations. FBS spoofs the network broadcast parameters, such as SIB1, TAC, PLMN ID, and PCI. It can selectively drop messages like Msg1 and Msg3. The adversary exploits the fact that the number of UE retries depends on the preambleTransMax parameter, which is shared via SIB1 [5] by the base station. The adversary sets a significantly high value to this parameter to engage the UE in the connection setup loop. UEs cannot verify preambleTransMax before attempting the RACH procedure. The objective of FBS in this threat model is to deny 5G services to the legitimate UEs by keeping them in an end-less loop of RACH failures. Note that the FBS lacks UE credentials (stored in SIM) and therefore it cannot complete the registration process.

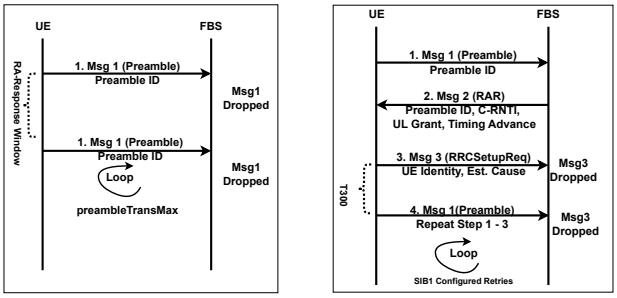
Based on the assumptions given above, UE, while in its mobile state, performs handover operations. It attempts to camp on a new base station, which could be an LBS or an FBS. The handover to an LBS follows the standard mechanism, allowing the UE to continue its operations seamlessly.

C. DoS Attacks on 5G RAN

The DoS attacks are based on the premise that the UE has camped onto an FBS due to radio link failures or weaker signal strength from the LBS. The FBS is capable of conducting the following attacks:

a) RACH Procedure Drop: The adversary broadcasts the initial broadcast messages, including SIB1, by impersonating an LBS. The MAC layer of UE initiates RACH procedure, constructs and forwards a message to the PHY layer, which is transmitted to the FBS as Msg1. The FBS drops the Msg1, causing the UE to revert to the RRC_IDLE state. The UE waits for the raResponseWindow and re-initiates the RACH procedure at the next opportunity as seen in Fig. 3a. This procedure repeats until the retries reach the preambleTransMax threshold. As this value was spoofed, it keeps UEs engaged for a longer duration, leading to DoS attacks.

b) RRC Setup Request Drop: Fig. 3b shows the call-flow of this attack. Following the initial RACH procedure, the UE proceeds with the RRC Setup phase. Using information received in the RACH Response (Msg2), the UE generates and transmits the RRCSetupRequest, commonly referred to as (Msg3). The FBS can exploit this step by dropping the Msg3 and thereby preventing the setup process from progressing. As a result, the UE reverts to the RRC_IDLE state and re-attempts the entire RACH procedure after the expiration of T300 timer. The number of retries depends on the SIB1 configuration advertised by the FBS.



(a) RACH Procedure Drop (b) RRC Setup Request Drop

Fig. 3: DoS Attacks on 5G RAN

III. Detection Technique

The 3GPP specs do not specify any technique for detecting FBS [5]. It is an implementation decision to either apply a policy mechanism or threshold-based detection at the UEs. Therefore, we set a threshold value t to restrict the number of retries. The detection algorithm runs at the UEs and is designed to be lightweight, monitoring key parameters such as TAC, PLMN ID, and PCI, as shown in Algorithm 1. The condition to flag a base station as FBS is based on the t value. These values can be collated as part of the measurement report [5] generated by the UE and shared with the attached LBS later.

IV. Experimental Setup and Data Collection

The experiments in this work will focus on UE-side FBS detection.

A. Proof Of Concept

A close to real-world PoC is setup using an Open Air Interface (OAI)-based 5G network, with a USRP x410 serving as the LBS. We refer to this as setup-A for our reference. The system was hosted on a Dell Optiplex 5080 workstation equipped with an Intel i7-12700 CPU and 16GB of RAM, running Ubuntu 22.04 OS. The 5G Core Network (5GC) was configured in a sandboxed containerized

Authorized licensed use limited to: Parul Institute of Engineering and Technology. Downloaded on September 15,2026 at 17:47:27 UTC from IEEE Xplore. Restrictions apply.

Algorithm 1 FBS UE Detection

Require: Retry threshold t
$msg1_retry_count \leftarrow 0$
$msg3_loop_count \leftarrow 0$
while RRC connection not established **do**
    Send Msg1 (PRACH preamble)
    if Msg2 (RAR) is received **then**
        Send Msg3
        Start T_{300} timer
        if Msg4 is received before T_{300} expiry **then**
            Connection established; reset all counters
        else
            $msg3_loop_count \leftarrow msg3_loop_count + 1$
            $msg1_retry_count \leftarrow 0$
            if $msg3_loop_count \geq t$ **then**
                Flag **FBS impacting Msg3**
                Prepare Measurement Report; **break**
            end if
        end if
    else
        $msg1_retry_count \leftarrow msg1_retry_count + 1$
        if $msg1_retry_count \geq t$ **then**
            Flag **FBS impacting Msg1**
            Prepare Measurement Report; **break**
        end if
    end if
end while

environment, and docker-compose was used for orchestration of the services. For the UE, we used three `Google Pixel 5` devices to establish legitimate registration and PDU sessions with the 5G network.

1) Normal case: Another setup also included an `OAI-based` 5G network with `USRP x410`, as an additional base station with similar system configurations as `setup-A`. We refer this as `setup-B`. This was kept at a distance from the previous one. This was done to emulate the characteristics of a weaker signal as the distance from the device increases. One of the UEs, connected to the `setup-A`, was moved away, and the `USRP x410`, belonging to `setup-A` was switched off, emulating the loss of signals, eventually bringing the UE to `RRC_IDLE` state. The UE was then physically brought closer to `setup-B`. This allowed the UE to attempt RRC procedure with this setup. As the `setup-B` base station used parameters identical to those of `setup-A`, except for the PCI, the UE was able to camp on this setup, complete registration successfully, and establish data connectivity. This helped us demonstrate the case of UE handover to an LBS in the event of a loss of radio link from its attached base station.

2) FBS case: To emulate the FBS scenario, a similar setup like `setup-A` was utilized. We refer to it as `setup-E`. We made a change by deleting the UE-specific registration details from the core service, such as AuthenticationInfo (E.g., `IMSI`, Key), and SessionManagementInfo (e.g., `NSSAI`) in UDR. This allowed the `setup-E` to act as an FBS, where the PLMN values enabled the UE to engage in the registration process but resulted in registration failures. This was demonstrated by allowing the UE to move away from `setup-A` and switching off the `USRP x410` of `setup-A`, resulting in a radio failure. The UE, in `RRC_IDLE` state, received broadcast messages `MIB/SRB1` from `setup-E`, and attempted `RACH` procedure followed by `RRCSetup`. However, due to an authentication failure, the registration was unsuccessful.

This proof of concept (PoC) successfully demonstrated the FBS attack. However, due to hardware limitations, detailed data collection, particularly from the lower layers of a commercial mobile device, was not feasible. To address this, we modified the setup and included a `USRP x410` as the UE to enable fine-grained data collection of lower layers, such as PHY and MAC. The revised setup is explained in the following section.

B. Attack Emulation - Simulated UE

Emulating the attack scenarios: To emulate the attack scenarios, we modified the scheduler program for the RAN node (DU). We modified the code to ensure dropping of i) `RACH Msg1` and ii) `RRCSetup` request `Msg3`, both originating from the UE. The modified code is made available for further research [15]. This modification of the code was enabled with the help of an additional change in the config file of gNB, as shown in Listing 1, to avoid frequent code changes in the scheduler program. Here, value zero represents the normal case, and value one represents the attack case.

```
MACRLCs=(
{
    ...
    ...
    fbs_enable                      = 1;
    msg1_drop_enable                = 1;
    msg3_drop_enable                = 0;
    msg1_display_enable             = 1;
    msg3_display_enable             = 0;
    ...
}
```

Listing 1: Config File Modification

1) Emulating RACH drop: As described in the previous section, the parameter `msg1_drop_enable` is set to 1, and we observe the following at the UE (Listing 2). Observations indicate that the UE failed to receive the `RAR`, suggesting that the FBS dropped the `Msg1` to keep the UE engaged in the procedure. We utilize the threshold `t` with varied values to restrict the number of RACH procedures initiated from the UE.

2) Emulating RRCSetup Request drop: Similarly, to emulate the RRCSetup Request drops, the parameter `msg3_drop_enable` is set to 1 in the DU configuration, and we observe the following at the UE (Listing 3). In this scenario, the UE successfully receives the Random Access Response (`RAR` or `Msg2`) from the gNB, following which the MAC layer constructs and transmits the `Msg3`. After

Authorized licensed use limited to: Parul Institute of Engineering and Technology. Downloaded on September 15,2026 at 17:47:27 UTC from IEEE Xplore. Restrictions apply.

```
[NR_MAC] PRACH scheduler: Selected R0 Frame
    333, Slot 19, Symbol, Fdm 0
[PHY] PRACH [UE 0] in frame. slot 333.19,
    placing PRACH in position 2828, Msg1/MsgA-
    preamble frequency start 0 (k1 0),
    preamble_offset 8, first_nonzero_root_idx
    0, preambleIndex=43
[MAC] [UE 0] RAR reception failed
[MAC] [UE 0] RAR reception failed count: 3
[MAC] mac->mib_ssb:0
[NR_MAC] PRACH scheduler: Selected R0 Frame
    335, Slot 19, Symbol, Fdm 0
[PHY] PRACH [UE 0] in frame. slot 335.19,
    placing PRACH in position 2828, Msg1/MsgA-
    preamble frequency start 0 (k1 0),
    preamble_offset 8, first_nonzero_root_idx
    0, preambleIndex=15
[MAC] [UE 0] RAR reception failed
[MAC] [UE 0] RAR reception failed count: 4
[MAC] mac->mib_ssb:0
```

Listing 2: RACH Drop as seen at the victim UE

transmission, the UE awaits the `Msg4` within a predefined timeout period. As `Msg3` is dropped by the FBS, the UE waits until `T300` and restarts the `RACH` procedure. The proposed detection algorithm, running locally at the UE, monitors the number of failed `Msg3` retransmissions and raises the FBS flag when the retransmissions exceed `t`, preventing prolonged engagement with a potential FBS. This information is collated to generate a measurement report for sharing with an LBS later.

```
[NR_MAC] [UE 0][RARPROC][RA-RNTI 010f] Got BI
    RAR subPDU 5ms
[NR_MAC] [UE 0][RARPROC][RA-RNTI 010f] Got
    RAPID RAR subPDU
[NR_MAC] [UE 0][RARPROC][626.7] Found RAR with
    intended RAPID 48
[MAC] received TA command 42
[NR_MAC] [RARPROC][626.17] RA-Msg3 transmitted
[NR_MAC] [RARPROC][627.17] RA-Msg3
    retransmitted
[NR_MAC] [RARPROC] Count of RA-Msg3
    retransmitted 0, cellid: 0
[NR_MAC] [RARPROC][628.17] RA-Msg3
    retransmitted
[NR_MAC] [RARPROC] Count of RA-Msg3
    retransmitted 1, cellid: 0
[NR_MAC] FBS Detected, Msg3 Restransmissions
    exceeded 2, cellid: 0
[MAC] [UE 0] Contention resolution failed
```

Listing 3: RRCSetup Drop as seen at the victim UE

C. Data Collection

We employed a simulated testbed to carry out our data collection, featuring a split CU/DU architecture alongside a simulated UE, all built using the OAI RAN stack (`nr-softmodem`) v2.5.0. The primary objective was to assess resource consumption across both normal and attack scenarios. By comparing CPU and memory usage in legitimate connections versus FBS conditions, we were able to quantify the extent of resource wastage caused by such attacks. This setup provided a controlled yet realistic environment for evaluating the performance and impact of FBS-related threats on network elements.

To simulate realistic and unpredictable UE behavior, we set up an experiment involving three distinct scenarios: normal operation, RACH drops, and RRCSetup Request drops. On the gNB side, we prepared separate configuration files for each scenario and used an automated script that sequentially launched the `nr-softmodem` with respective configuration. This script ensured that each run was terminated before the next began, effectively emulating UE mobility between an LBS and a FBS.

On the UE side, another script was used to monitor resource consumption. This script continuously ran the UE process and captured real-time CPU and memory usage using the `top` command. It remained active as long as the UE process was running, recording system performance for each scenario. While the gNB randomly selected one of the three configurations for each cycle, the UE-side script ensured that the resource usage data was logged accurately for all the three scenarios.

Each configuration was executed for 60 seconds, and the entire cycle was repeated 10 times. This coordinated setup between the gNB and UE enabled us to collect consistent and realistic performance metrics across various network scenarios, while still preserving an element of randomness in the test environment.

V. Result and Discussion

We demonstrate the resource drain caused by unsuccessful connection attempts of the victim UE to a fake base station. As shown in Fig. 4, the CPU consumption without a detection technique does not bring any threshold scenario. This indicates that the FBS can exploit substantial UE resources despite the absence of a successful connection. However, when threshold-based detection is used, CPU consumption is reduced, demonstrating a decrease in CPU resource utilization.

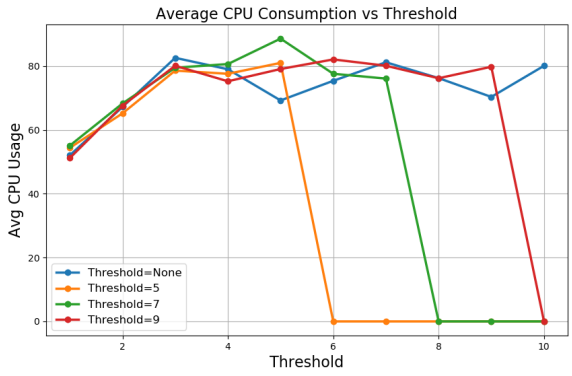


Fig. 4: Average CPU Consumption

The experimental results provided data for FBS evaluation on the UE side, including RRC failures, RACH failures, and

Authorized licensed use limited to: Parul Institute of Engineering and Technology. Downloaded on September 15,2026 at 17:47:27 UTC from IEEE Xplore. Restrictions apply.

increased CPU consumption of the victim UE observed during attack scenarios. Notably, DoS attacks aimed at lower layers, such as PHY and MAC, consume fewer resources compared to attacks targeting the NAS layer [14]. This economical resource usage for lower-layer attacks is attributed to fewer message exchanges and the absence of cryptographic protections. In contrast, the NAS layer attacks require the attacker to participate in more signaling handshakes and process additional control messages as part of the RRC procedures. These findings, coupled with the UE's geo-location, can be integrated into measurement reports of UEs during connection establishment with an LBS later for aiding the mobile operators in identifying the presence of fake base stations in their networks.

VI. Conclusions

The work emphasized the critical importance of addressing FBS attacks at layer 2 in 5G RAN. We established the scenario of FBS attacks occurring at this layer and provided a practical demonstration to highlight the vulnerabilities and impact of such attacks. To counter these threats, we proposed a UE-side detection mechanism that leverages a threshold-based retry mechanism, designed to identify indicative patterns of FBS scenarios effectively. Detecting attacks at the lower layers enables much faster root cause analysis, reducing the need to escalate detection to upper layers and thereby improving overall response efficiency. Building upon this foundation, the future direction of our work aims to incorporate scenarios involving faulty base stations, broadening the scope to include both malicious and misconfigured entities. The detailed measurement reports generated from our detection mechanism offer valuable insights that mobile operators can utilize to implement sophisticated detection logic as part of O-RAN RICs (RAN Intelligent Controllers), enabling real-time monitoring, analysis, and mitigation within programmable network environments.

Acknowledgments

This work is partially supported by the ISEA Phase-III project, titled 'Security in Distributed Wireless Networks', funded by MeitY, Govt. of India, and by the DST-FIST grant.

References

[1] A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5g network with the advent of 6g: Architecture and emerging technologies," *IEEE Access*, vol. 9, pp. 67 512–67 547, 2020.

[2] J. Sasiain, D. Franco, A. Atutxa, J. Astorga, and E. Jacob, "Toward the integration and convergence between 5g and tsn technologies and architectures for industrial communications: a survey," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 1, pp. 259–321, 2024.

[3] M. Mahyoub, A. AbdulGhaffar, E. Alalade, E. Ndubisi, and A. Matrawy, "Security analysis of critical 5g interfaces," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 4, pp. 2382–2410, 2024.

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

[5] "3gpp ts 38.300, nr; overall description; stage-2," 3rd Generation Partnership Project (3GPP), Tech. Rep. TS 38.300, March 2023, release 17. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.300/

[6] "3gpp ts 24.501, non-access-stratum (nas) protocol for 5g system," 3rd Generation Partnership Project (3GPP), Tech. Rep. TS 24.501, March 2023, release 17. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/24_series/24.501/

[7] E. Bitsikas, S. Khandker, A. Salous, A. Ranganathan, R. Piqueras Jover, and C. Pöpper, "Ue security reloaded: Developing a 5g standalone user-side security testing framework," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023, pp. 121–132.

[8] K. Samin Mubasshir, I. Karim, and E. Bertino, "Gotta detect'em all: Fake base station and multi-step attack detection in cellular networks," *arXiv e-prints*, pp. arXiv–2401, 2024.

[9] S. Kriaa, A. Feki, S. Papillon, T. Chene, and I. Ouattara, "Detecting fake base stations using knowledge graphs and ml-based techniques," in *Proceedings of the IEEE Virtual Conference on Communications (VCC) 2023*. IEEE, 2023, pp. 37–42.

[10] H. Wen, P. Porras, V. Yegneswaran, A. Gehani, and Z. Lin, "5g-spector: An o-ran compliant layer-3 cellular attack detection service," in *Proceedings of the 31st Annual Network and Distributed System Security Symposium, NDSS*, vol. 24, 2024.

[11] M. Saedi, A. Moore, P. Perry, and C. Luo, "Rbs-mlp: A deep learning based rogue base station detection approach for 5g mobile networks," *IEEE Transactions on Vehicular Technology*, 2022.

[12] J.-H. Huang, S.-M. Cheng, R. Kaliski, and C.-F. Hung, "Developing xapps for rogue base station detection in sdr-enabled o-ran," in *Proceedings of the IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2023, pp. 1–6.

[13] T. Heijligenberg, D. Rupprecht, and K. Kohls, "The attacks aren't alright: Large-scale simulation of fake base station attacks and detections," in *Proceedings of the 17th Cyber Security Experimentation and Test Workshop*, 2024, pp. 54–64.

[14] N. Ludant, M. Vomvas, and G. Noubir, "Unprotected 4g/5g control procedures at low layers considered dangerous," *arXiv preprint arXiv:2403.06717*, 2024.

[15] A. K. Subudhi, "OAI_USRP_IITH: Implementation of oai with usrp at iith," https://github.com/Ashitkumarsubudhi/OAI_USRP_IITH, 2025, gitHub repository.

Authorized licensed use limited to: Parul Institute of Engineering and Technology. Downloaded on September 15,2026 at 17:47:27 UTC from IEEE Xplore. Restrictions apply.