An Experimental Study of Denial of Service Attacks on a 5G COTS Hardware

Karim Baccar, Abdelkader Lahmadi

An Experimental Study of Denial of Service Attacks on a 5G COTS Hardware

Karim Baccar* and Abdelkader Lahmadi*
*Université de Lorraine, CNRS, Inria, LORIA, 54000 Nancy, France
karim.baccar@inria.fr, abdelkader.lahmadi@loria.fr

***Abstract*—While a significant efforts have been made in the specification and deployment of the 5th generation mobile systems (5G), there is a noticeable lack of practical experiments regarding its security. The 3GPP standardisation body has already defined numerous protocols, procedures and implementation guidelines for 5G. However, many of these requirements and procedures are missing assessment and experiments to validate their security conformance. In this paper we experiment and implement various DoS attacks in the 5G protocol stack by using a COTS 5G solution. we mainly show through these experiments that numerous potential misconfiguration and misuses pose significant threats to the security of 5G networks.**

***Index Terms*—5G protocols, 5G Security, DoS, attacks**

I. Introduction

Mobile networking has witnessed remarkable progress and changes, especially with the introduction of 5G. Since 2016, the 3GPP standardisation body has been working on the development of the 5G technology and published three main releases namely the release 15, 16 and 17. These releases have brought significant improvement to mobile networking and have expanded the range of applicability of mobile networking to different business and sectors, many of them are critical. The complexity of the 5G infrastructure and protocols however widened considerably the attack surface of the network and increased its complexity creating therefore a plethora of attack scenarios that can potentially compromise the whole network.

The 3GPP specification TS 33.501 [1] details the main security requirements related to 5G mobile networks. The standard mentions enhanced security against International Mobile Subscriber Identity(IMSI) catching with the use of Subscription Concealed Identifiers(SUCI) during initial registration and beamforming inherent protection against sniffing attacks. However according to the work of Chuan et al. [2], in which the authors studied the feasibility of 4G attacks in 5G, they demonstrated that 5G networks are still vulnerable to some of the attacks of its predecessor. This is mainly due to a lack of security of the messages that are prior to the creation of the security context and to the fact that security features are still optional at the user and control planes. As an example TS 33.501 requirements related to message confidentiality and integrity mentions that confidentiality protection of user data is optional to use in the network, integrity protection is also is optional for the user plane and mandatory for only specific messages in the control plane. Threats similar to RRC-storm DoS attacks are therefore still exploitable in the 5G network but they were only experimented in LTE networks. [3]. Certain functionalities in the 5G NR network can also create a potential security risk especially if they are omitted or misconfigured by MNO's during network deployment. The emergency procedure as an example has been the subject of multiple research studies regarding its potential security risk. While still being a legislative requirement, the potential misuse of the emergency procedure can lead to a number of attacks such as SIP emergency session suppression, overbilling attacks, PWS messages spoofing and suppression [4], [5]. With the wide availability of Software Defined Radios(SDR) devices, the potential security risk that telecommunication infrastructure is subject to is constantly increasing and its impact can target critical infrastructure especially in the case of 5G. This work presents an experimental analysis on novel Denial-of-Service attacks against different layers of the 5G protocol stack; this provides a better analysis on the impact and the cost effectiveness of 5G NR attacks. We will test the attacks using a B210 SDR and Commercial off the Shelf (COTS) 5G NR base station.

The remainder of this paper is organized as follows. Section II provides p reliminaries and background elements of the 5G protocol stack, procedures and relevant gNb timers. Section III presents the attack scenario and the architecture of our testbed. Section IV will be dedicated to an analysis of the experimental results and will include configuration recommendations to mitigate the attacks. Finally section V concludes the paper.

II. Preliminaries

3GPP brought with 5G NR a multitude of changes to the protocol and procedures necessary to meet the novel requirements of enhanced Mobile Broadband (eMBB), massive Machine Type Communications (mMTC) and Ultra Reliable Low Latency Communications (URLLC). The new use cases changed drastically the way telecommunication networks can be used and deployed.

In this section we will present some of the relevant protocols and procedures, namely the protocol stack used in 5G Radio Access Network (RAN), the different types of registration procedures and their main functionalities.

A. Protocol Stack

The 5G NR architecture specifies a set of protocols for the control and user planes. The establishment and management of sessions and the authentication procedures happen at the **Non-Access Stratum layer** (NAS) of the control plane. The

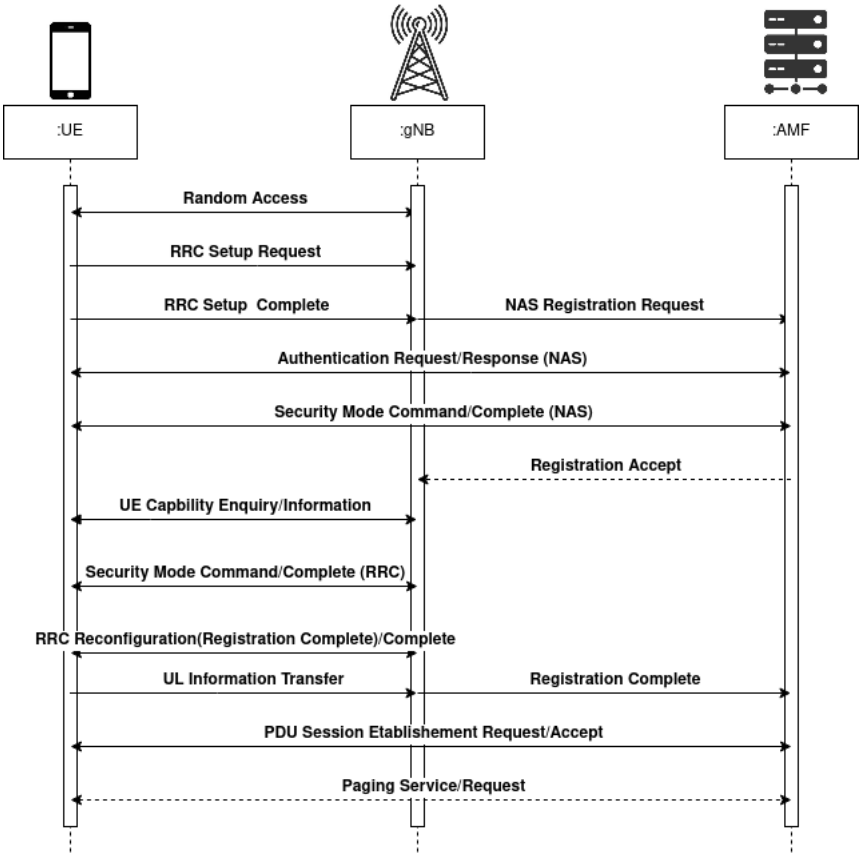

Fig. 1: Overall steps of the registration procedure of a UE in a 5G mobile network.

Radio Resource Control (RRC) is used to exchange control information with the device to initiate the parameters of the radio sessions. The primary services of RRC include the broadcast of system information related to NAS and AS, Paging, security key function management, management of radio bearers, mobility function management, QoS management, UE reporting and encapsulation of NAS messages. Protocols of layer 2 include **Radio Link Control** (RLC), **Packet Data Convergence Protocol** (PDCP), and **Medium Access Control** (MAC) and provide roles that includes ciphering, QoS flow management, mapping between logical and transport channels, protocol error detection and resegmentation, segmentation. Layer 1 includes the PHY layer responsible for demodulation, modulation of physical channels and frequency and time synchronization for control and user planes.

Communication between the **Access and Mobility Function** (AMF) and the gNB occurs at the N2 interface which transports NGAP protocol messages encapsulated within **Stream Control Transmission Protocol** (SCTP). The NG Application Protocol has two main sets of services, UE-associated services which are responsible for the communication between the core network and the UE and Non UE-associated services related to the management of the RAN node itself.

The user plane also includes the **Service Data Adaptation Protocol** (SDAP) responsible for the management the Qos of the data and for encapsulating user data. This data can be **Session Initiation Protocol** (SIP) packets directed to the IMS, internet or intranet services.

B. UE Procedures

1) Initial Registration: Figure 1 details the registration procedure of a UE in the 5G network. First the UE synchronizes with the gNB in order to obtain an uplink Common Control Channel (CCCH), thereafter, the UE initiates the RRC Setup Request message, this is called the *Random Access* procedure. Secondly, after sending RRC Setup Complete in the RRC Connection Procedure, the UE is able to communicate with the AMF over the Dedicated Control Channel (DCCH). Thirdly, after sending the registration request message over the NAS protocol, the UE solves the authentication challenge that is sent to it and then negotiates the security algorithms that will be used during the connection with the AMF. Finally, after setting up the security configuration in AS and NAS, the UE is then able to initiate a PDU session request with NAS to the AMF in order to receive an uplink data session.

2) Emergency Registration: Depending on local regulations and operators policies it is also possible for an unauthenticated UE to access the network with solely the IMEI, this is in the context of an emergency registration. It is used mostly when the UE requires emergency PDN connectivity or IMS calls but is not subscribed to the MNO's network, example

services can be emergency services such as rescue services or the police. Depending on the operators configuration the UE will be in a limited state and therefore usual services will not be available. However, gaining access to the network with the emergency procedure forces it to adopt a null scheme security level where no integrity or confidentiality protection of the messages will be used, communication can therefore be spoofed and eavesdropped by adversaries.

In our context, emergency procedure can be a way of obtaining core resources from the network such as PDU sessions without having valid a SUCI identifier, this will be used to setup the DoS attacks that are detailed in section IV.

III. Experimental Testbed

In this section we will present our experimental testbed architecture [6] and its different components, the configuration parameters that we adopted for the callbox and the modification that we made on the srsRAN library.

A. Testbed Architecture

The main component of our testbed is the base station which is able to provide RAN functionalities and integrates also a core 5G server. We make the choice to use a commercial off-the-shelf base station that offers a full-stack 5G network. The second main component of our experimental testbed is the UE emulator. We chose to use the srsUE tool which is able to provide a 5G NR UE modem implemented entirely in software. This tool is implemented in C++ and is actively maintained by an open source community, it also supports multiple SDR cards including USRP B2x0/X3x0 families, BladeRF, LimeSDR. The wireless communications between the srsUE and the Amarisoft Box are realized through the Ettus USRP B210 SDR card as described in Figure 2.

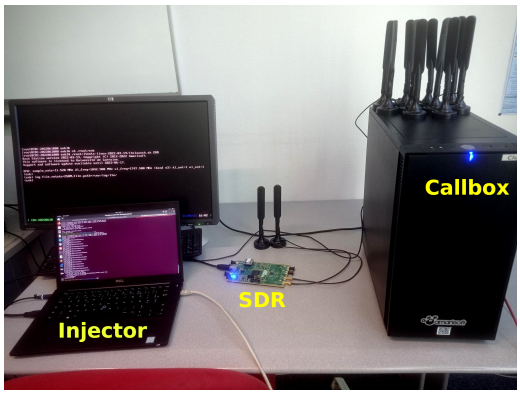

Fig. 2: The experimental setup of our testbed including the Amarisoft call Box (base station), the SDR card Ettus USRP B210 connected to a laptop running with srsUE.

B. Amarisoft Callbox Configuration

Amarisot Callbox is a commercial solution for testing 5G features, it includes an embedded base station and supports standalone(SA) and non-standalone(NSA) 5G architectures. It acts as a 3GPP compliant all-in-one 5G station and offers the possibility to realize conformance and functional testing on most of the existing features that 5G offers. The capacity of the callbox is rather extensive as it supports up to 500 simultaneous UE connection, up to 75 mbs uplink, MIMO and is 3GPP release 17 compliant. The configuration that we applied on the callbox was based on the requirements for the attack scenario and also the compatibility between srsUE and the callbox. Table I represents a subset of the parameters that we adopted for the callbox.

TABLE I: A subset of the configuration parameters used for the Amarisoft Callbox.

Parameters	Value
EIA Modes	NIA0,NIA1,NIA2
EEA Modes	NEA0,NEA1,NEA2
Inactivity timer	3 minutes
T3512	54min (Default)
FR1 band	Band 3

For the confidentiality and integrity protection for both Access Stratum (AS) and Non Access Stratum (NAS) communication, we enabled null security with NIA0 and NEA0 algorithms, this still complies to a real case scenario as it was proven by the work of Chlosta et al. [7] that certain MNO's do enable null security algorithms in deployment networks. We also have AES and Snow 3G based algorithms that are adopted by NIA1,NIA2 for integrity protection and NEA1 and NEA2 for the confidentiality protection. The frequency band that will be adopted in our test environment will be NR band 3 which works on 1785 Mhz on uplink and 1805 Mhz on downlink, this frequency range is reliable and enough for the test cases that will be adopted given that we wont require much bandwidth resources.

The T3512 timer is responsible for timing the periodic registration procedures of the UE. This procedure is used over 3GPP access to periodically notify the availability of the UE to the network. During an emergency session and on the expiry of the timer, the AMF will locally deregister the UE from the network as specified by TS 124.501 [8] in 10.2, the default value of this timer according to the specification is 54 minutes.

C. srsRAN Library

srsRAN [9] is an open sourced software suite that offers implementations of LTE and NR components that are compliant to the 3GPP standard. The project includes a full NR implementation with the RAN and core server. In our work, we only rely on the srsUE since the gNB and core network components are already provided by the Amarisoft callbox.

srsUE program provides the main functionalities that a commercial 5G modem can offer, this includes the Non-Standalone (NSA) and Standalone (SA) support, handover, QoS support and PDU session establishment. The library is written in C++. Our first task was to identify the role of the program classes and their interactions.

The class */srsue/src/ue.cc* represents a concrete implementation of the UE and contains methods related to disabling/enabling and initiating the UE. It also includes an

instance of */srsue/src/stack/ue_stack_lte.cc*, which is used for the management of NR procedures and the instanciation of each layer of the NR stack. It also allows the initiation of the RRC and NAS procedures at the class code available in */srsue/src/stack/rrc_nr/rrc_nr.cc* and */srsue/src/stack/upper/nas_5g.cc*. These classes contain methods that includes sending PDU's to lower layers and instantiating NR messages.

IV. DoS Attacks Implementation and Experimentation

In this section we will demonstrate the technical feasibility of 5G attacks using openly available resources, this in order to better assess the impact of such attacks and to mitigate potential risks. Our adversary models are based on DoS attacks on three protocols used in 5G NR networks, namely RRC, NAS and SIP protocols. We will therefore present for each attack scenario its implementation and its possible mitigation methods.

A. RRC-storm Attack

The purpose of the RRC-storm attack is to generate fake RRC connection requests in order to the deplete the pool of RRC sessions of the Callbox. This attack has been seen and tested in previous generation networks; the RRC protocol in addition did not see much changes when it comes to the RRC connection procedure as the initial message are still unprotected and vulnerable. Our goal is to therefore test the feasibility of the attack in a 5G environment.

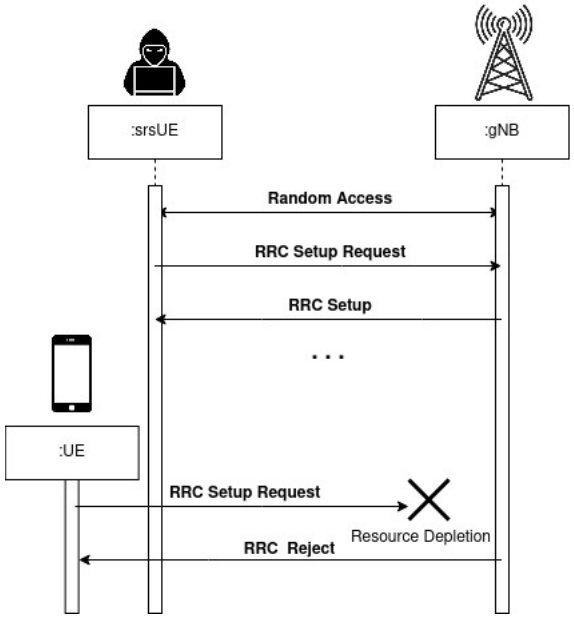

Fig. 3: Flow diagram showing the RRC-storm attack.

1) Adversary Model: The attacker using an SDR device will repeatedly perform the *Random Access* procedure in order to consume RRC resources. After reaching its maximum capacity of simultaneous RRC connections, the gNb will start rejecting legitimate RRC requests. The impact of this attack will depend on the configuration of the inactivity timer. In optimal cases and with enough resources the attacker can cause a denial of service against the base station. Figure 3 details the procedure of the RRC-storm scenario.

2) Implementation: For this DoS scenario, we repeat the *Random Access* procedure by overriding the instanciation of the UE object in the */srsue/src/stack/rrc_nr/main.cc* class. After optimizing the library for the DoS use case, we managed to get 3 procedures per second. The inactivity timer of the callbox was set to 3 minutes.

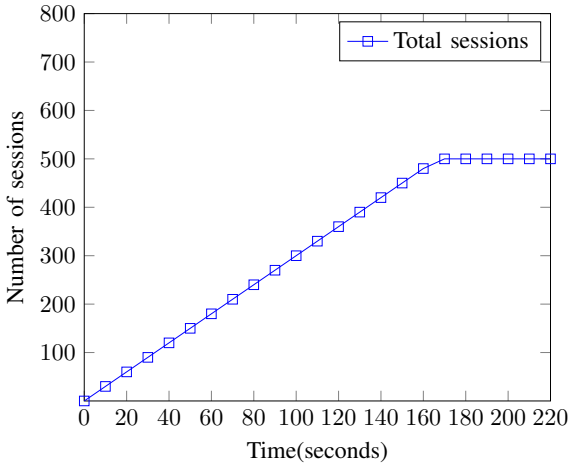

Fig. 4: The gradual increase of the number of RRC sessions during the RRC-storm attack.

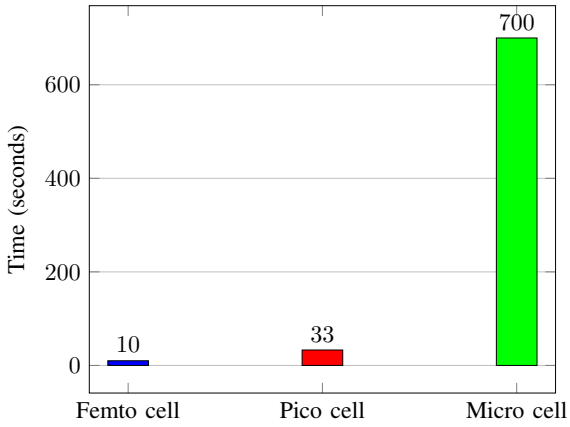

Fig. 5: Estimated time to saturate a gNodeB based on each cell type.

3) Validation: Using the modified srsUE library, we flooded the Amarisoft callbox with fake RRC Requests. Our modified version of srsUE is able to process 3 RRC connections per second, the callbox supports 500 simultaneous UE. After 3 minutes, the callbox started rejecting newer RRC Request messages. Figure 4 details the evolution of active RRC connection after launching the DoS attack. Figure 6 shows the message received in Amarisoft log after the maximum pool

of connection is reached. In order to assess the impact of this attack on 5G deployment cell types, figure 5 represents an estimation of the time required to saturate the most common 5G cell types. Femto cell are mostly used in small personal indoor deployments and support only 16 users. Pico cells support up to 64 users and micro cells up to 2000 users [10]. The saturation time however still depends on the configuration of the RRC inactivity timer for each cell where high values are most vulnerable.

1	CCCH-NR	RRC setup request
1		RRC setup request: maximum number of UEs or bearers reached in the cell
1	CCCH-NR	RRC reject

Fig. 6: RRC log following the RRC-storm denial of service.

4) Mitigation: The main mitigation technique for RRC-storm based attacks as seen in previous generation networks rely mostly on fine tuning the inactivity timer configured for the gNb. Setting this timer to a minimal value can mitigate resource depletion but this will increase however the control traffic congestion within the network. Randomizing the inactivity was also found to be a proved solution [3]. Detection can also be done through traffic analysis of the number of RRC Connection compared to NAS connections as this latter is necessary for authenticating the UE and for PDU session allocation. Unusual unbalance is therefore an indicator of a network problem. Figure 7 shows the type of messages sent during the attack, we can observe an overwhelming number of RRC Connection requests compared to NAS messages, this is also confirmed by figure 8 which details the CPU consumption of the callbox during the attack. We can notice the difference between the AMF and the gNb CPU usage, the AMF being almost idle.

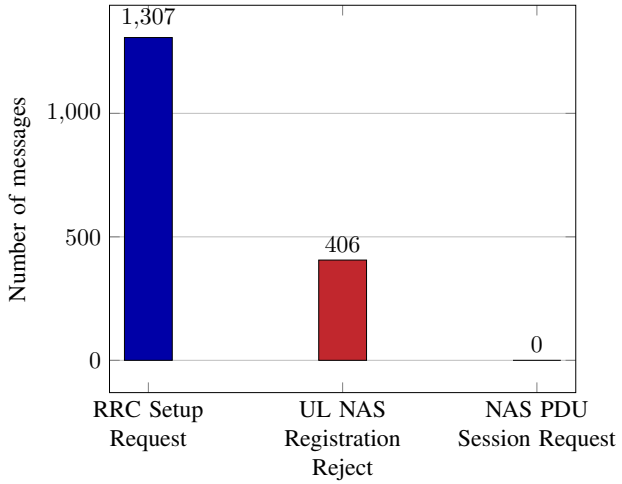

Fig. 7: Type of messages sent during the RRC-storm attack.

B. PDU Resource depeletion

The goal of this attack is to deplete the allocated IP addresses pool for PDU sessions. The emergency registration can be used maliciously for this purpose in order to allocate PDU sessions by requesting emergency PDU sessions repeatedly.

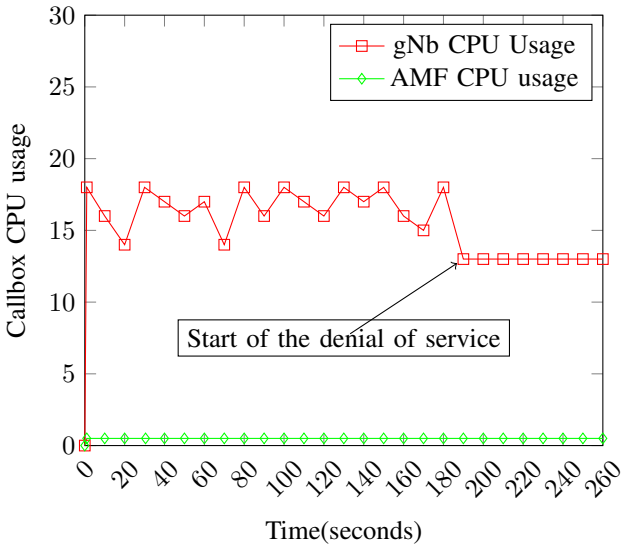

Fig. 8: CPU consumption during the RRC-storm attack for the gNb and AMF components.

1) Adversary Model: The attacker will flood the callbox with emergency registration. As the emergency connection based on the IMEI is completely anonymous, we can launch this procedure repeatedly and therefore consume core resources at will. Each registration will have a PDU resource allocated to it that consists in an IP address for the duration of the T3512 timer. PDU resources provide end-to-end user plane connectivity and is necessary to access the Data Network (DN). These resources if depleted will bare legitimate access to the DN. The impact of the depletion depends on the internal configuration of the AMF, if emergency PDU resources are independent of normal PDU resources only the emergency plane will be affected. Otherwise, the denial of service will also affect normal connections. Figure 9 details the procedure of the IP depletion scenario.

2) Implementation: Our first modification was to add the emergency registration procedure to the UE, we added a new parameter in the configuration file *emergency_registration_5g* that enables emergency IMEI based registration of UE's. We also added a new service request procedure that comply to the requirement of 3GPP during the initiation of an emergency PDU session. We also modified the UE object in order to continuously reboot itself and perform the registration procedure for the DoS scenario.

3) Validation: We flooded the callbox with emergency registrations. Our srsUE registration procedure takes approximately 5 seconds. After 40 minutes The experimentation resulted in barring access to PDU sessions for the emergency plane only. Figure 11 shows the number of IP addresses depleted over time, after reaching 500 IP addresses the Callbox started rejecting PDU session requests as shown in figure 10.

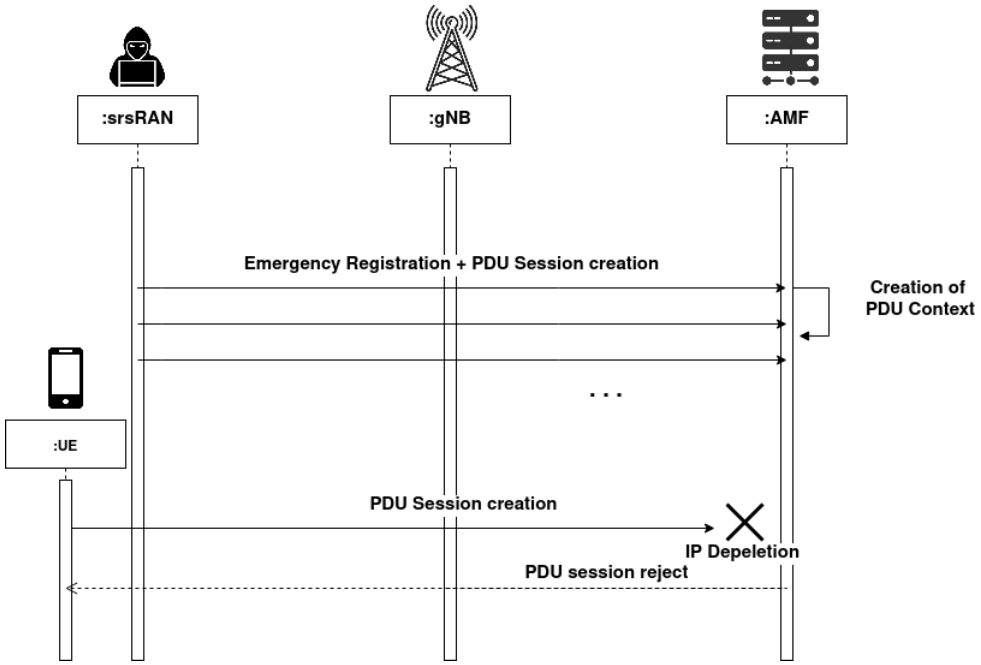

Fig. 9: Flow diagram showing the IP depletion attack.

NAS	103 (100)	5GMM	UL NAS transport
NAS	103 (100)	5GSM	PDU session establishment request
NAS	103 (100)		Can't allocate new IPv4 address

Fig. 10: Callbox logs showing PDU resource depletion.

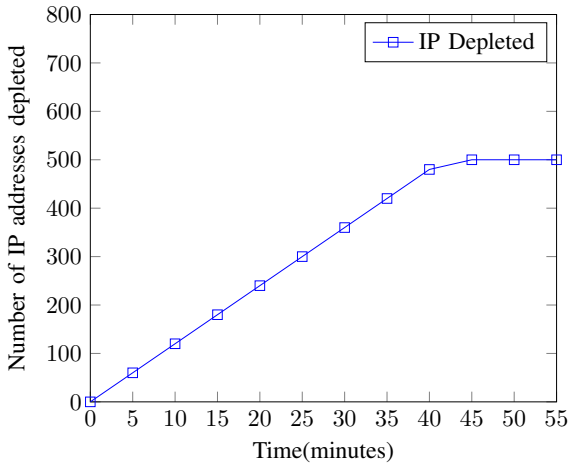

Fig. 11: Number of IP addresses depleted over time.

4) Mitigation: The 3GPP specification does not specify regulation concerning the usage of the PDU resources in emergency sessions and therefore it is up to local policies to whether allow emergency PDU sessions or not. This has shown to be a potential vulnerability for DoS attacks on PDU resources. A suggested recommendation for this attack if regulation mandates emergency anonymous registration is to check the validity of the IMEI during registration, if the IMEI is unknown to the Equipement Identity Register(EIR), emergency services should not be granted.

C. Telephony DoS on VoNR

The telephony DoS (TDoS) attack is a well-known attack of telecommunication networks and 5G networks are still however vulnerable to it. The attack consists in flooding public safety services with fake calls that are automatically generated. This will result in an overwhelming number of inbound malicious calls that can be disruptive to critical services such as the public safety response systems. In 5G networks the main components responsible for VoNR calls is the IMS.

1) Adversary Model: The attacker using an SDR device and a 5G modem will first initiate emergency registration to the target network then will initiate anonymous SIP calls to emergency services. The main objective of this attack is to make emergency services unavailable to legitimate users, this attack can be particularly disruptive in case of public emergencies. The attack mainly targets the IMS component of the network responsible for the management of VoNR calls.

2) Implementation: Our first modification consisted in modifying the the PDU session establishment procedure in order to offer VoNR features. We also modified the NAS 5G procedures in */srsue/src/stack/upper/nas_5g.cc* in order to initiate a SIP session following the allocation of the PDU session to the UE. The initiation of the SIP session was based on the tool called "SIPP", we used the tool to send a SIP invite message to the emergency number that is already predefined in the Amarisoft callbox, this procedure was then continuously repeated.

3) Validation: We flooded the callbox with anonymous SIP calls directed to the IMS component, we mainly targeted the

emergency SIP service available by default in the callbox. We successfully flooded the service by initiating fake SIP sessions to the emergency number using NR emergency procedure. Figure 12 shows 10 concurrent ghost sessions initiated with the IMS component of the Amarisoft callbox. Figure 13 details the IMS log of the callbox during the attack, anonymous users are created and SIP VoNR are initiated.

```
[10] Dialog Anonymous <=> service:sos
- State: init
- Type: echo
- Qos: pending
- Timeout: 26.0
- audio: RTP=10018/192.168.4.38:40002, rx=0, tx=0
         RTCP:10019/192.168.4.38:40003, rx=0, tx=0
         sendrecv
         Qos pending
- Duration: 0.0s
```

Fig. 12: Amarisoft Callbox IMS interface showing 10 concurrent ghost SIP sessions.

SIP	1		INVITE	urn:service:sos SIP/2.0 from 192.168.4.2:5060
IMS				Create anonymous
RX				127.0.1.100:3868 AA-Request
SIP	1		SIP/2.0	100 Trying to 192.168.4.2:5060
SIP	1		SIP/2.0	183 Session Progress to 192.168.4.2:5060
RX				127.0.1.100:3868 AA-Answer
SIP	2		INVITE	urn:service:sos SIP/2.0 from 192.168.4.6:5060
IMS				Create anonymous
RX				127.0.1.100:3868 AA-Request
SIP	2		SIP/2.0	100 Trying to 192.168.4.6:5060
SIP	2		SIP/2.0	183 Session Progress to 192.168.4.6:5060
RX				127.0.1.100:3868 AA-Answer
SIP	3		INVITE	urn:service:sos SIP/2.0 from 192.168.4.10:5060
IMS				Create anonymous
RX				127.0.1.100:3868 AA-Request
SIP	3		SIP/2.0	100 Trying to 192.168.4.10:5060
SIP	3		SIP/2.0	183 Session Progress to 192.168.4.10:5060
RX				127.0.1.100:3868 AA-Answer

Fig. 13: Amarisoft Callbox log showing SIP sessions being initiated repeatedly.

4) Mitigation: Mitigating a SIP based TDoS attack will depend on the internal configuration of the IMS component. Embedded SIP analytics to detect malicious behaviour can be used, in this case the IMS can temporarily blacklist SIP source addresses responsible for the attack. In the case of an emergency SIP call, anonymous calls will be temporarily disabled. Another method to mitgiate this attack will be to enable vocal CAPTCHA based challenges to verify if the caller is human or not.

D. Discussion

The attacks that we implemented and experimented are carried on a COTS callbox. Although it implements most of the existing 5G features and is compliant to the 3GPP specification, its capacity does not translate to a deployment grade node. Such hardware, especially macro nodes, will therefore require more resources and fine tuning of srsRAN library in order to implement the described attacks to a real case scenario. The goal of this work is therefore to mainly demonstrate common exploitable vulnerabilities in 5G RAN that are not vendor dependent. The attacks that we have presented are based on inherent design and feature flaws in the specification of the NR protocols.

V. Conclusion

In this paper, we experimented and analyzed the impact of DoS attacks on a COTS base station and we found that 5G networks are still vulnerable to attacks targeting both RAN and core resources. We presented DoS attacks on the RRC protocol with the RRC-storm attack, on the NAS protocol with PDU depletion based on emergency sessions and on the IMS services with the SIP TDoS attack. We also detailed recommendations in order to mitigate such scenarios. In future work, we plan to evaluate more attacks on 5G including false messages and data injection.

Acknowledgement

This work is partially supported by 5G events Lab, the project IMPACT DigiTrust of "Lorraine Université d'Excellence" and by EU H2020 project AI@EDGE(101015922).

References

[1] 3GPP, "Security architecture and procedures for 5g system, technical report 33.501."

[2] C. Yu, S. Chen, F. Wang, and Z. Wei, "Improving 4g/5g air interface security: A survey of existing attacks on different lte layers," *Computer Networks*, vol. 201, p. 108532, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621004576

[3] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the untouchables: Dynamic security analysis of the lte control plane," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1153–1168.

[4] Y. Hu, M.-Y. Chen, G.-H. Tu, C.-Y. Li, S. Wang, J. Shi, T. Xie, L. Xiao, C. Peng, Z. Tan, and S. Lu, "Uncovering insecure designs of cellular emergency services (911)," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, ser. MobiCom '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 703–715. [Online]. Available: https://doi.org/10.1145/3495243.3560534

[5] E. Bitsikas and C. Pöpper, "You have been warned: Abusing 5g's warning and emergency systems," in *Proceedings of the 38th Annual Computer Security Applications Conference*. ACM, dec 2022. [Online]. Available: https://doi.org/10.1145/3564625.3568000

[6] K. Baccar and A. Lahmadi, "An experimental testbed for 5g network security assessment," *IEEE/IFIP Network Operations and Management Symposium*, 2023.

[7] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, "Lte security disabled: Misconfiguration in commercial networks," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 261–266. [Online]. Available: https://doi.org/10.1145/3317549.3324927

[8] 3GPP, "Non-access-stratum (nas) protocol for 5g system (5gs);."

[9] srsRAN. [Online]. Available: https://github.com/srsran/srsRAN

[10] A guide to 5g small cells and macrocells. [Online]. Available: https://www.essentracomponents.com/en-us/news/industries/telecoms-data/a-guide-to-5g-small-cells-and-macrocells