2022-12

IDENTIFICATION AND ANALYSIS OF ATTACKS USING RECOVERED RADIO NETWORK TEMPORARY IDENTIFIERS ON 5G USER EQUIPMENT

Schindler, Thomas M.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IDENTIFICATION AND ANALYSIS OF ATTACKS USING RECOVERED RADIO NETWORK TEMPORARY IDENTIFIERS ON 5G USER EQUIPMENT

by

Thomas M. Schindler

December 2022

Thesis Advisor: Britta Hale
Co-Advisor: Chad A. Bollmann

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE IDENTIFICATION AND ANALYSIS OF ATTACKS USING RECOVERED RADIO NETWORK TEMPORARY IDENTIFIERS ON 5G USER EQUIPMENT	**5. FUNDING NUMBERS**
6. AUTHOR(S) Thomas M. Schindler	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The next cellular network, 5G, will drastically increase the number of devices on a network. The increase in devices will provide a bigger attack surface for potential intruders and offer a pivot point to get inside networks once exploited. Researchers have already discovered how to de-anonymize the messages in the physical downlink control channel to recover Radio Network Temporary Identifiers (RNTI). Analysis of the 5G protocols identified potential vulnerabilities when an RNTI is known. A potential attacker is now able to recover RNTIs, making attacks on 5G devices inevitable. Additional research conducted into protocol vulnerabilities was completed and found possible vulnerabilities in some of the 5G protocols. This thesis examined how the aggregated results of prior work can be utilized to attack individual pieces of user equipment. Cyber security professionals will benefit from this research by understanding how these attacks will be carried out in order to identify defenses against them.

14. SUBJECT TERMS 55G, Man-in-the-Middle, MiTM, Cellular-Radio Network Temporary Identifier, C-RNTI, Denial of Service, DoS, Subscription Permanent Identifier, SUPI	**15. NUMBER OF PAGES** 71
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

IDENTIFICATION AND ANALYSIS OF ATTACKS USING RECOVERED RADIO NETWORK TEMPORARY IDENTIFIERS ON 5G USER EQUIPMENT

Thomas M. Schindler
Major, United States Army
BS, Franklin University, 2011
MS, University of Maryland, University College, 2016

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Approved by: Britta Hale
Advisor

Chad A. Bollmann
Co-Advisor

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The next cellular network, 5G, will drastically increase the number of devices on a network. The increase in devices will provide a bigger attack surface for potential intruders and offer a pivot point to get inside networks once exploited. Researchers have already discovered how to de-anonymize the messages in the physical downlink control channel to recover Radio Network Temporary Identifiers (RNTI). Analysis of the 5G protocols identified potential vulnerabilities when an RNTI is known. A potential attacker is now able to recover RNTIs, making attacks on 5G devices inevitable. Additional research conducted into protocol vulnerabilities was completed and found possible vulnerabilities in some of the 5G protocols. This thesis examined how the aggregated results of prior work can be utilized to attack individual pieces of user equipment. Cyber security professionals will benefit from this research by understanding how these attacks will be carried out in order to identify defenses against them.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

5G-GUTI 5G Global Unique Temporary Identifier

5G-TMSI 5G Temporary Mobile Subscriber Identity

ABBA Anti-Bidding down Between Architectures

AES Advanced Encryption Standard

AES Advanced Encryption Standard

AMF Access and Mobility Management Function

ARPF Authentication credential Repository and Processing Function

AUSF Authentication Server Function

AUTN AUthentication TokeN

C-RNTI Cell Radio Network Temporary Identifier

CRC Cyclic Redundancy Check

DCI Downlink Control Information

DoS Denial-of-Service

FBS False Base Station

GCI Global Cable Identifier

GLI Global Line Identifier

gNB 5G Base Station

GUAMI Globally Unique Access and Mobility Management Function (AMF) Identifier

HPLMN Home Public Land Mobile Network

HRES Hash RESponse

HXRES Hash eXpected RESponse

I-RNTI Inactive Radio Network Temporary Identifier

IMSI International Mobile Subscriber Identity

MAC	Message Authentication Code
MCC	Mobile Country Code
MitM	Man-in-the-Middle
MNC	Mobile Network Code
MSIN	Mobile Subscriber Identification Number
NAS	Non-access Stratum
PDCCH	Physical Downlink Control Channel
PDCP	Packet Data Convergence Protocol
PHY	Physical
PLMN	Public Land Mobile Network
RAND	Random Number
RAP	Random Access Procedure
RES	RESponse
RG	Residential Gateway
RLC	Radio Link Control
RNTI	Radio Network Temporary Identifier
RRC	Radio Resource Control
SDAP	Service Data Adaptation Protocol
SEAF	Security Anchor Function
SIDF	Subscription Identifier De-concealing Function
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TC-RNTI	Temporary Cell Radio Network Temporary Identifier
UDM	Unified Data Management
UE	User Equipment
USIM	Universal Subscriber Identity Module
XRES	eXpected RESponse

Acknowledgments

First and foremost I would like to thank my wife, Lisa, and my two daughters, Bella and Mari. I greatly appreciate your support and encouragement throughout this process. Thank you and I am deeply grateful.

I would also like to thank my advisors, Dr. Britta Hale, Dr. John Roth, and CDR Chad A. Bollmann. Your patience and support are appreciated. Thank you for guiding me on this path.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

Cellular networks use identifiers to communicate with devices authorized to use the network. The network needs to have a way to identify a device that belongs on the network and those that do not. The identity can be permanent or temporary. A unique identity is needed to ensure that only authorized users are on the network. The temporary identity allows the permanent identity to remain protected. Standards were implemented to protect the permanent identities from observation by malicious actors.

Previous versions of the cellular network used the International Mobile Subscriber Identity (IMSI). The networks passed the International Mobile Subscriber Identity (IMSI) in plain-text, providing little protection to the identity of the subscriber. The 5G standard changes the identity to a Subscription Permanent Identifier (SUPI), which before being transmitted over the network is encrypted to become a Subscription Concealed Identifier (SUCI). The change protects the identify of the subscribers by sending only the encrypted SUCI over the network. More is discussed about the SUPI and SUCI in Chapter 2.

This thesis looks at the use of Cell Radio Network Temporary Identifiers (C-RNTIs) of 5G devices to deliver attacks to a specific device. The C-RNTI is another temporary identity used by the base station at the Radio Resource Control layer to ensure that user equipment receives their messages. The C-RNTI is anonymized in the headers of downlink control information messages. and this provides a low level of security from an attacker discovering the C-RNTI. In recent research, a method was discovered that broke the encoding of the Downlink Control Information (DCI) messages and allows a passive observer or malicious actor to obtain the C-RNTI [1]. The thesis researches possible ways the C-RNTI can be used to target a device.

1.1 Motivation

The next generation cellular network, 5G, will drastically increase the number of devices on a network as possible targets for malicious actors. In addition to cellular devices, 5G will increase the number of smart refrigerators, toasters, lights, and other devices connected in

a smart home. Another area which 5G will enable is smart transportation where communication will happen vehicle-to-vehicle, vehicle-to-sensors, and vehicles-to-people [2]. All of these devices pose as a potential attack point to penetrate a network and need to be secured.

Several research papers investigated different security issues with 5G implementation and protocols. One research paper looked at the vehicle to everything communication (VFX) made possible with 5G technology and the security concerns with 5G that would affect these communications [2]. The concerns addressed included trust, security, and privacy issues. Some of the biggest concerns included impersonation, Man-in-the-Middle (MitM), and replay attacks. All of these would disrupt the communication between devices or between devices and people causing confusion and potential physical harm.

One report stated that surveys taken from 2017 to 2019 showed that there are many security and privacy concerns over the adoption of 5G [3]. One concern includes the potential weakness of security on the network edges in comparison to the core network [3]. Another issue is the introduction of Software Defined Networks, Artificial Intelligence, and Machine Learning creating security flaws that attackers can exploit [3]. Potential security flaws in 5G have already been identified and it is just a matter of time before they come under attack [4].

The objective of this work is to understand possible attacks that utilize C-RNTIs and effects of these attacks on 5G devices. Understanding how the devices and protocols are affected will allow us to develop tools to identify attacks and potential defenses against these attacks. This thesis explores the feasibility and difficulty of the attacks.

1.2 Thesis Organization

The reminder of the thesis is organized as follows. Chapter 2 gives an overview of the 5G architecture, protocols, procedures, and identifiers that are discussed in the thesis. Chapter 3 discusses related work including research on the decoding of DCI messages and vulnerable points in the protocols and procedures. Chapter 4 builds on both of these previous works by looking at combining them to attack a device. The necessary steps are described. Chapter 5 contains the conclusion and discussion of future work

CHAPTER 2:
Background

The 5G network increases the capabilities and number of devices able to connect and utilize the cellular network. The increase arises from new technology and utilization of the millimeter-wave portion of the electromagnetic spectrum. Security becomes more challenging as the number of devices on the network increases. Each new device becomes a potential target for a malicious actor.

Some background is necessary for understanding parts of the discussion later in the thesis. This chapter will provide an overview of the 5G architecture, identifiers, authentication, and vulnerable procedures. The main identifier discussed is the C-RNTI and how it can be utilized to target single devices. In addition to the C-RNTI, the thesis looks at the SUPI and its exposure to place a permanent identity on a piece of user equipment. Two parts of authentication are discussed: The first is the key derivation, to demonstrate the complexity of deriving the key used for integrity protection and enciphering of communications between the base stations and user equipment. The second part includes authentication of a piece of user equipment to the network. In the last portion of this chapter, we discuss the procedures that are vulnerable to some level of attack utilizing the C-RNTI.

2.1 5G Architecture

A high-level overview, shown in Figure 2.1, depicts how older generations of cellular networks can overlap with 5G networks. The older generations of cellular networks operate between 450 MHz to 6 GHz [5]. Frequencies above 24 GHz complement these lower frequencies to create a heterogeneous network [5]. Macrocells utilize the low frequencies that previous generations used below 6 GHz to provide the widest coverage. Smaller cells utilize the higher frequencies, providing less coverage while increasing bandwidth. The introduction of much smaller cells will make a very dense network able to support the Internet of Things, device-to-device, and machine-to-machine communications [6]. The density of base stations will reduce the load and latency. Ultimately, the architecture creates more serving cells, which in turn allows more devices on the network.

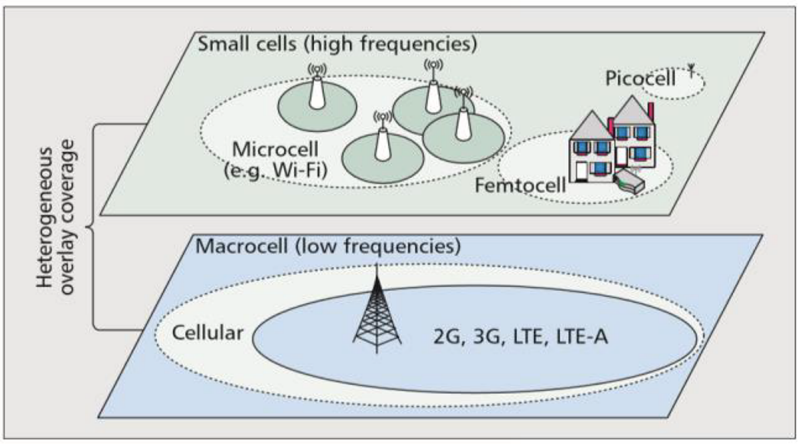

Figure 2.1. Comparison of cell sizes in a 5G network. Source: [7].

The main takeaway from this section is that there will be an increase in the number of base stations in an area. The addition of base stations increases the capacity of the network. The serving cells are much smaller for the high frequencies utilized in the upper range of the 5G network. A device establishes secure communications to the network through an authentication procedure.

2.2 Authentication

The 5G networks handle authentication through two methods, AKA and 5G-EAP. One difference between the two revolves around the key derivation process for each. The User Equipment (UE) and core network derive their keys separately to ensure that a key used for integrity protection or ciphering is not sent or passed between the devices. This practice prevents an attacker from discovering the current key that is being utilized. The main take away from this section is the complexity of the key derivation process and brief introduction of the authentication procedure. The attacks discussed in Chapter 4 do not interfere with these processes other than preventing it from fully completing.

2.2.1 Key Derivation

The network and user equipment derive the same keys to be used with the ciphering and integrity protection algorithms in order to protect the confidentiality and integrity of the

data. The keys are derived separately by the network and the user equipment. The derivation of the keys starts during the authentication process.

User equipment contains a secure piece of hardware called the Universal Subscriber Identity Module (USIM) that stores the long-term subscription key (K), the home network public key, the home network public key identifier, and protection scheme identifier [8, p. 27]. The USIM generates the CK (Cipher Key) and the IK (Integrity Key) to send to the mobile equipment during the authentication and agreement procedure [8, p. 52]. The UE derives the K_{AUSF} key from those keys as well as the Serving Network Name and the sequence number XOR'ed with the AK [8]. The serving network name is used again with the K_{AUSF} to derive the K_{SEAF} key. The K_{SEAF} along with the SUPI and Anti-Bidding down Between Architectures (ABBA) is used in the key derivation function to get the K_{AMF} key. The next derivation function utilizes the K_{AMF} and the Non-access Stratum (NAS) uplink counter to derive the K_{gNB} [8]. Figure 2.2 depicts the derivation of keys used for encrypting and integrity protection within the user equipment (mobile equipment in the diagram) [8, p. 48].

The network derives the keys in similar fashion; however, the long-term key is stored in the Unified Data Management (UDM) or Authentication credential Repository and Processing Function (ARPF). The different keys are stored in the respective network nodes, for example the K_{AMF} is stored in the network Access and Mobility Management Function (AMF). The keys are derived and stay in the Home Public Land Mobile Network (HPLMN) until the K_{SEAF} is derived and sent to the serving network's Security Anchor Function (SEAF) node [8, p. 48]. The K_{gNB} is sent to the serving base station for the final encryption and integrity protection keys can be derived [8, p. 49].

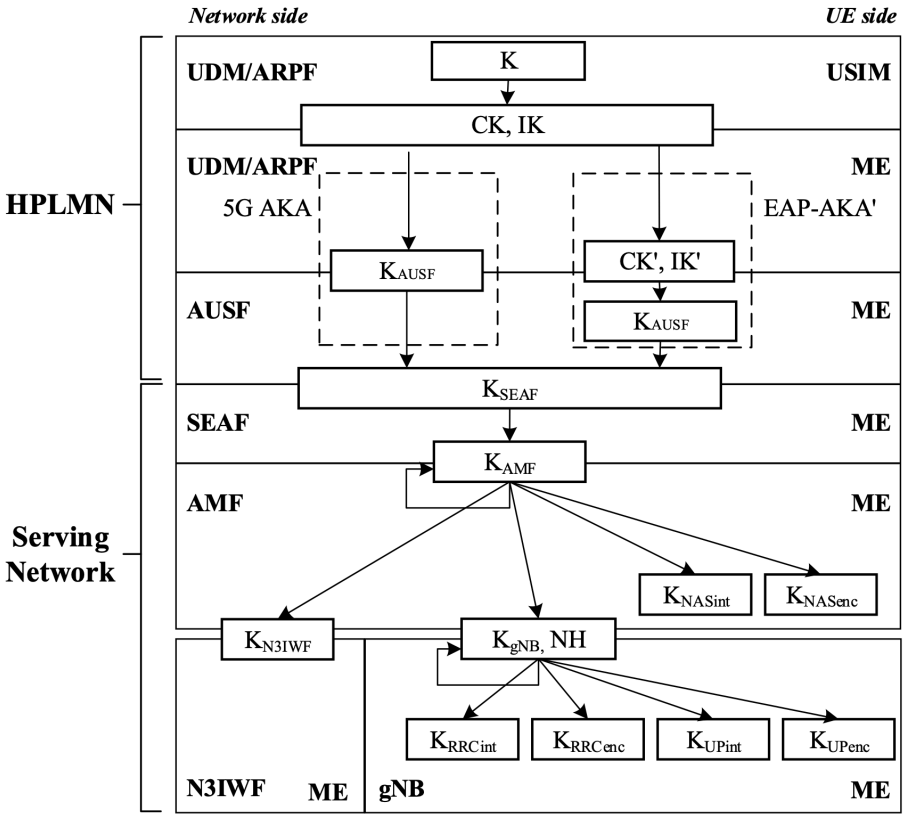

Figure 2.2. Key derivation in the user equipment and network. Source: [8, p. 48].

One important thing to note for future discussion is the use of the NAS Counters that are used to derive the K_{gNB}. If one of these is different from what the network uses, the derived keys will not match and therefore not work. The process will stop and have to be restarted. This is discussed in Chapter 4 Section 4.2.

2.3 Authentication Procedure

The authentication of the UE and network start with the user equipment sending the initial authentication request message containing the user equipment‘s SUCI or 5G Global Unique Temporary Identifier (5G-GUTI). The initial message is received by the serving network‘s SEAF node and then forwarded to the home network‘s Authentication Server Function (AUSF) node. The AUSF forwards the message to the UDM or ARPF. The SUCI is sent

to the Subscription Identifier De-concealing Function (SIDF) for de-concealment and to obtain the SUPI.

The UDM creates an authentication vector after receiving that message. The home environment authentication vector contains Random Number (RAND), AUthentication TokeN (AUTN), eXpected RESponse (XRES)*, and K_{AUSF}. The vector is sent to the AUSF. The AUSF derives the next key, K_{SEAF}, by inputted the K_{AUSF} and the serving network name into the key derivation function. The AUSF creates an authentication vector to send to the serving network's SEAF. The vector contains the RAND, AUTN, and Hash eXpected RESponse (HXRES)*, and K_{SEAF}. The serving network's SEAF creates the serving environment authentication vector with the RAND, AUTN, and HXRES*. The SEAF forwards the RAND and AUTN to the user equipment.

The user equipment's USIM calculates a RESponse (RES). The device sends the RES back to the serving network and calculates the K_{AUSF} and K_{SEAF}. The SEAF calculates the Hash RESponse (HRES)* and compares to the HXRES*. If the same, the SEAF sends the RES* to the AUSF. The AUSF compares the RES* and XRES*. If the same, the AUSF sends the SUPI and K_{SEAF} to the serving network's SEAF. Figure 2.3 summarizes this process. The input string for the RES* and XRES* include the following parameters: serving network name, length of serving network name, RAND, and length of RAND. The hashes of the response or expected response is the 128 least significant bits of the SHA-256 function output.

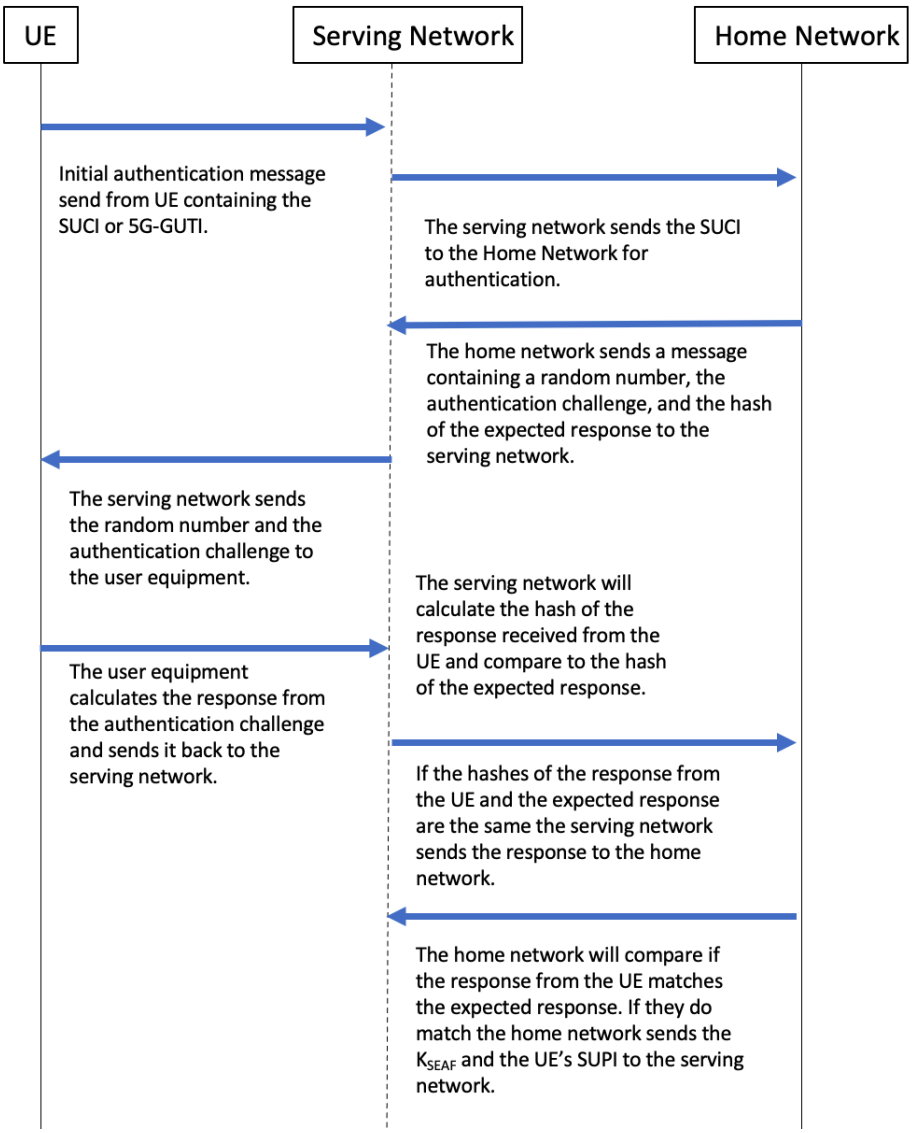

Figure 2.3. Authentication procedure. Adapted from: [8, p. 43].

After the user equipment is verified, both the serving network and user equipment further derive keys from the K_{SEAF}. The next key derived is the K_{AMF} and the key derivation function takes the K_{SEAF}, SUPI, and ABBA as parameters. The K_{gNB} key derivation function takes the NAS uplink counter along with the K_{AMF} to derive the key. From the K_{gNB} further keys are derived based on the algorithm used for the encryption and integrity protection.

2.4 Radio Resource Control and Non-access Stratum

Communication conducted between an end device and base station utilizes two protocol stacks. The two protocol stacks are divided into two groups called the user plane and control plane. The user plane handles the data that is being downloaded to a device or uploaded from a device. The control plane is responsible for the signaling information that establishes a connection to, authenticates, and informs user equipment. This plane uses unique identifiers for each piece of user equipment. An attacker requires the capture of these identifiers in order to conduct a targeted attack.

Figure 2.4 shows the control plane stack and its various layers. The NAS and Radio Resource Control (RRC) layers manage the connection setup, mobility, and security of the devices on the network [5]. The NAS layer‘s responsibilities include authentication and security. The NAS layer operates between the core network and the UE. The RRC protocol operates between the 5G Base Station (gNB) and the UE, and is where several of the vulnerabilities discussed in Chapter 3 are located. The layer handles the broadcast of system information, connection management, mobility functions, and handling of device capabilities. Analysis of these protocols discovered security flaws in both of these layers [4]. Chapter 3 discusses the security flaws in more detail.

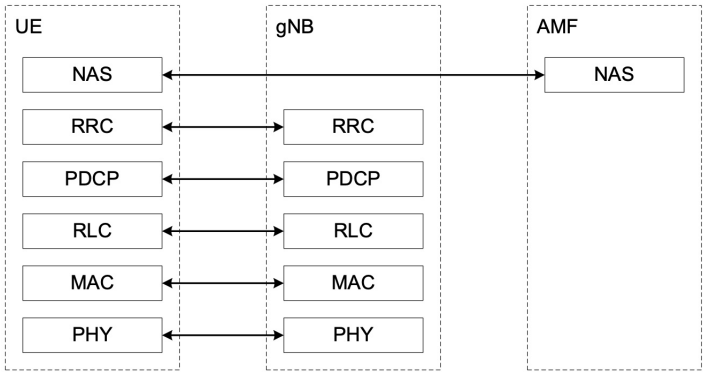

Figure 2.4. Protocol stack of the control plane. Source: [9, p. 21].

Figure 2.4 depicts the other sublayers in the control stack as well. The Physical (PHY) layer provides transport channels to the Message Authentication Code (MAC) sublayer [9, p. 39]. The MAC sublayer provides logical channels to the Radio Link Control (RLC) sublayer [9, p. 39]. The RLC sublayer provides RLC channels to the next higher sublayer [9, p. 39]. The Packet Data Convergence Protocol (PDCP) provides radio bears to the next sublayer [9, p. 39]. The Service Data Adaptation Protocol (SDAP) provides Quality of Service flows to the RRC layer [9, p. 39].

2.5 Procedures

This section covers the steps of the procedures discussed in the next chapters. The two procedures discussed in this thesis are radio setup and RRC security mode configuration. The initial RRC setup does not require integrity protection or ciphering during the initial setup. After the setup the device sends its SUCI as part of a registration requirement with the AMF. Upon successful completion of the registration, the base station will send the `RRC Security Command` message to determine what integrity protection and ciphering algorithms to employ [10, p. 60]. The algorithms include null protection, 128-bit SNOW 3G, 128-bit Advanced Encryption Standard (AES), and 128-bit ZUC [8, p. 36]. At the end of the security command procedure the UE and gNB have a secure connection with integrity protection and ciphering.

2.5.1 RRC Setup and Release Procedures

Radio setup procedure establishes a connection between gNB and UE. The whole connection establishment between the user equipment and base station is conducted prior to authentication and does not have integrity protection or ciphering [10, p. 51]. The procedure ends with the UE assigned a C-RNTI. The setup procedure starts with the UE sending a `RRC Setup Request` message to the gNB. The base station responds with either a `RRC Setup` or `RRC Reject` message to the UE. If the UE receives the setup message it will respond with a `RRC Setup Complete` message. The UE starts the process again if it receives the reject message. Figures 2.5 and 2.6 depict the procedure for a successful completion and a rejection [10, p. 53].

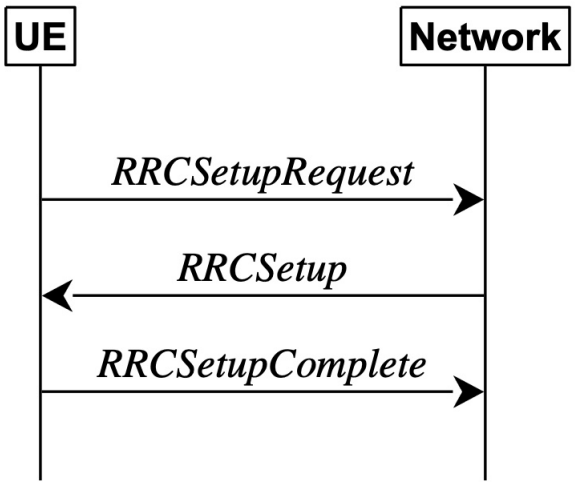

Figure 2.5. Steps of the RRC setup procedure. Source: [10, p. 53].

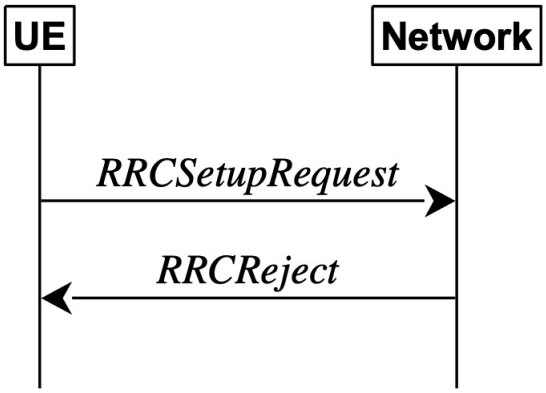

Figure 2.6. Protocol stack of the control plane. Source: [10, p. 53].

The `RRC Setup Request` message consists of two parts. The `UE-Identity` is either the previously assigned `5G-TMSI` (discussed in Section 2.6.2) or a random value between $1-2^{39}$, both are only 39 bits in length. The 5G Temporary Mobile Subscriber Identity (5G-TMSI) has to be assigned previously by an AMF. The `Establishment Cause` has several options depending on the requirements of the message: emergency, high-priority access, priority access, access, signaling, data, voice call, video call, SMS, and six spare variables for future use. The `RRC Setup Request` message is ended with a spare bit [10, p. 288]. This message travels from the UE to the network.

The `RRC Setup` message also consists of two main parts: `RRC Transaction Identifier` and `Critical Extensions`. The `Critical Extensions` only has two mandatory parts that are the `Radio Bearer Configuration` and `Master Cell Group`. Two optional fields are also available for non-critical and critical extensions [10, p. 285]. This message travels from the network to the UE.

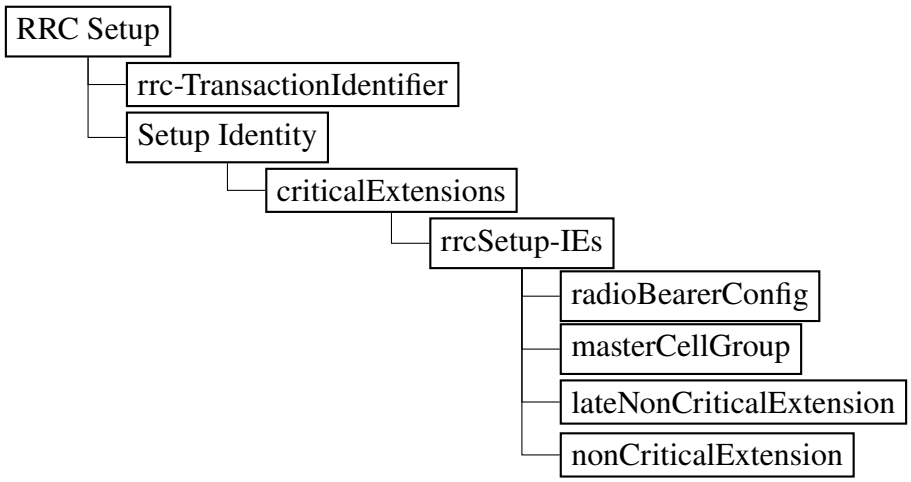

Figure 2.7. RRC Setup message contents Source: [10, p. 285].

Similarly, the `RRC Setup Complete` message consists of two parts, the `RRC Transaction Identifier` and the `Critical Extensions`. The transaction identifier is the same from the `RRC Setup` message. The `Critical Extensions` has two required components that are the `Selected PLMN-Identity` and the `Dedicated NAS-message`. The PLMN-Identity contains the Mobile Country Code and Mobile Network Code to identify the network that is used [11, p. 51]. There are six optional components of the `Critical Extensions` part of the setup complete message. Some optional components are the registered AMF, Globally Unique AMF Identifier (GUAMI)-Type, 5G-TMSI, late non-critical extensions, and non-critical extensions [10, p. 286].

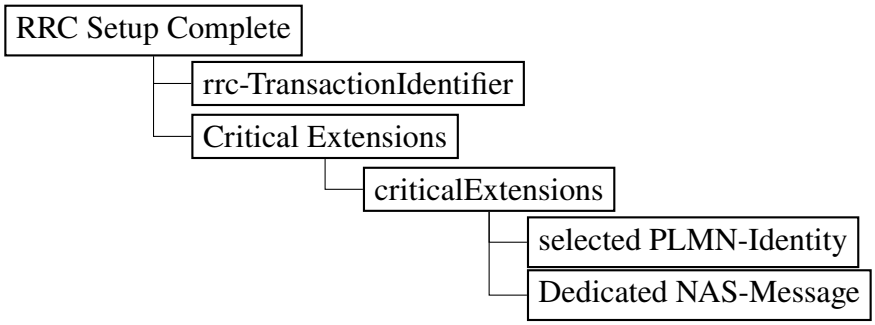

Figure 2.8. RRC Setup Complete message contents Source: [10, p. 286].

Figure 2.9 shows the variables within the RRC Setup Request message. The dotted line references the size of that part of the message. Figure 2.7 depicts the contents of the RRC Setup message sent from the network to the UE. The RRC Setup Complete message contents are shown in Figure 2.8.

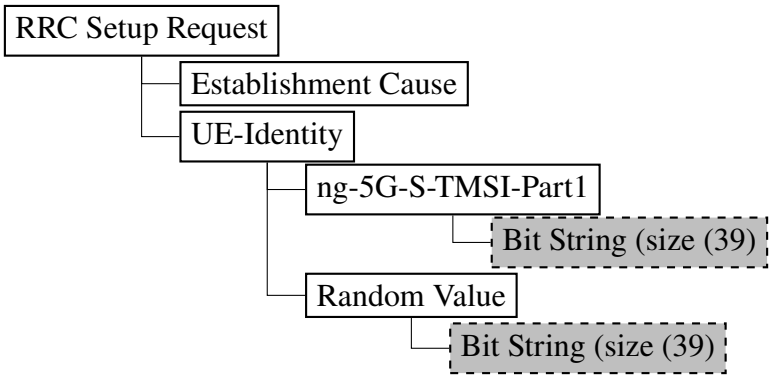

Figure 2.9. RRC Setup Request message contents. Source: [10, p. 288].

Figure 2.10 shows the procedure for the RRC Release message. The gNB utilizes this message to release the connection with the UE [10, p. 100]. The UE will be placed in the idle or inactive state when it receives this message. If security context (ciphering and integrity protection) has been established, the gNB transmits the RRC Release message with those protections [10, p. 908]. The message can be sent without the ciphering or integrity protection prior to their establishment between the UE and gNB.

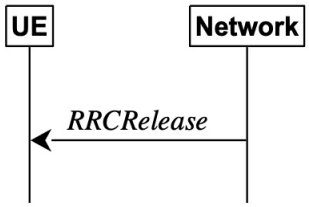

Figure 2.10. RRC Release procedure. Source: [10, p. 100].

2.5.2 RRC Security Mode

The next procedure discussed is the setup of the security mode for the Access Stratum. The procedure is started by the network sending a `Security Mode Command` message to the UE. The UE responds with one of two messages, `Security Mode Complete` or `Security Mode Failure`. After completion of the `Security Mode Command` message, integrity protection and ciphering are applied to future messages, except for the `Security Mode Complete` message; that message will only have integrity protection [10, p. 60]. If the UE fails to complete the command message it will use the previously configured settings for integrity protection and ciphering. On initial setup there is nothing previously established and the UE defaults to the null-scheme for integrity protection and ciphering [10, p. 51].

The `Security Mode Command` messages contains a transaction identifier and critical extensions and is shown in Figure 2.11 [10, p. 292]. The critical extensions contain the security configuration that the UE needs to apply [10, p. 292]. Both the `Security Mode Complete` and the `Security Mode Failure` contain the transaction identifier and the respective complete or failure message. Figures 2.12 and 2.13 depict the contents of the `Security Mode Complete` and the `Security Mode Failure` messages.

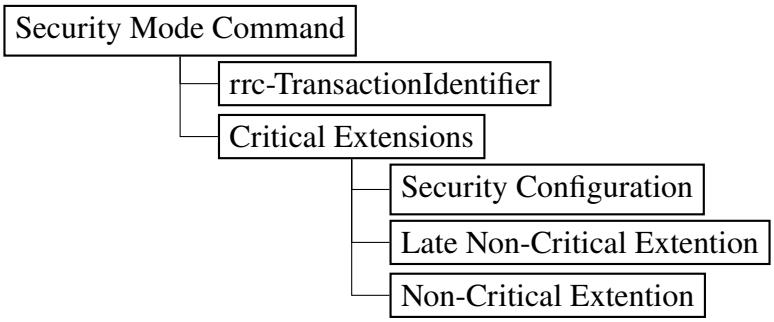

Figure 2.11. `Security Mode Command` message contents. Source: [10, p. 292].

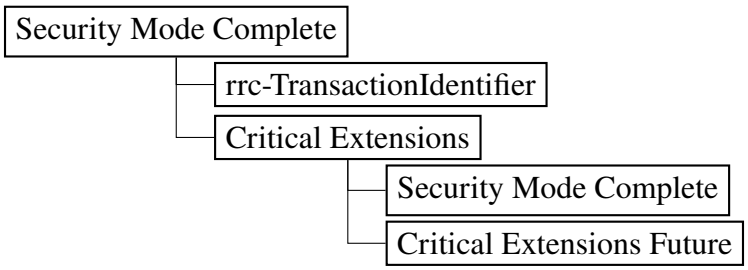

Figure 2.12. `Security Mode Complete` message contents. Source: [10, p. 293].

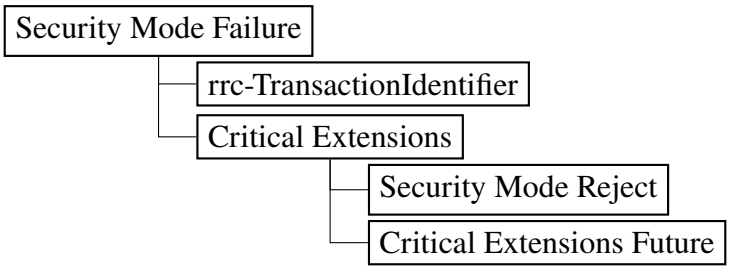

Figure 2.13. `Security Mode Failure` message contents. Source: [10, p. 294].

2.6 Identifiers

The 5G network uses identifiers for user equipment to ensure the devices are getting the data sent to them. The two primary identifiers this thesis looks at are the C-RNTI and SUPI in order to show that attacks can be targeted. C-RNTIs are used at the physical layer of the control plane protocol stack to ensure that the correct device only acts on messages in which it is the intended recipient. The primary purpose of the SUPI is identifying a device that is authorized to access the network or a servicing network the home network has agreements with. The C-RNTIs are temporary while the SUPI is a permanent identifier for the device.

2.6.1 Radio Network Temporary Identifier

Base stations and UEs utilize C-RNTI to ensure that only the intended recipient receives its traffic. The gNB assigns a C-RNTI to the UE within its cell and the C-RNTI is used to send information to the device and receive information from the device. In order to not

pass the C-RNTI in plain text, 5G encodes the C-RNTI into DCI messages along with error correction information [1]. The UE receives all the DCI messages in the cell and will decode these messages to see if the DCI message contains its assigned C-RNTI. If the device‘s assigned C-RNTI is in the control information message, the device processes that message and retrieves the control information. At any point that the decoded identifier does not match what the device was assigned, the device will stop decoding and move to the next DCI message [12].

A base station assigns the C-RNTI with the Random Access Procedure (RAP) when a device requests to establish a connection with the base station. The procedure involves four messages in a contention-based setting. The UE selects an available preamble and sends that to the gNB. The base station sends a response back that includes a temporary C-RNTI for the UE. The user equipment then sends the third message in the procedure back to the base station. The fourth message from the gNB includes the C-RNTI that the UE uses to identify the DCI messages that the device is required to act on [13].

User equipment maintains its C-RNTI unless the device moves out of the current serving cell, refreshed by the serving gNB, disconnects, or goes idle. When a device becomes idle it is assigned an Inactive Radio Network Temporary Identifier (I-RNTI) used in paging messages to alert the device to become active again [10]. Figure 2.14 illustrates the assignment of the C-RNTI and I-RNTI.

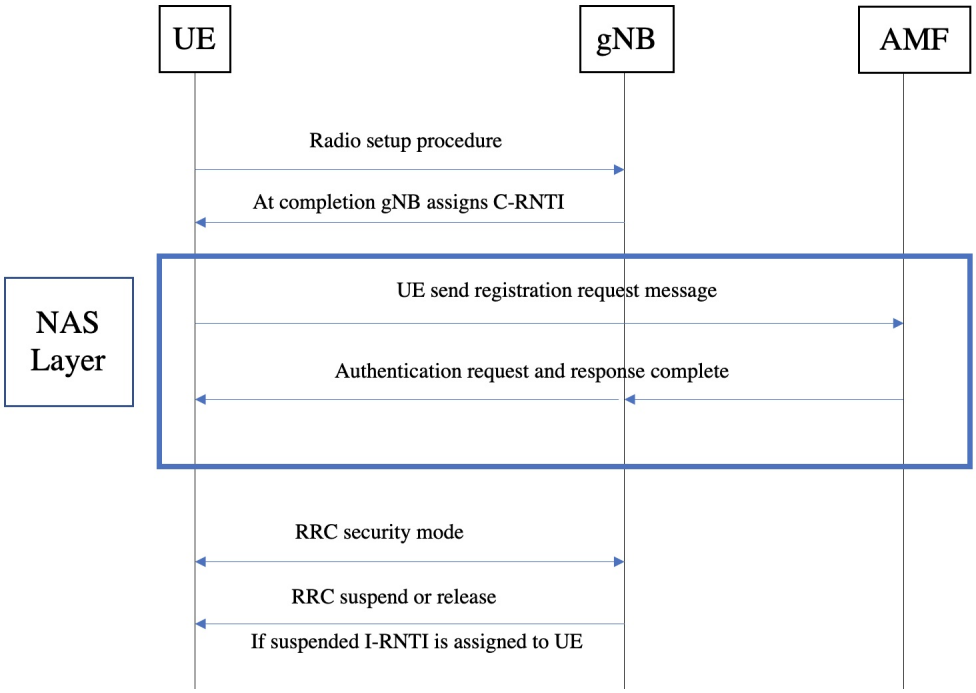

Figure 2.14. Procedures in C-RNTI assignment.

The UEs within the cell are required to decode DCI messages to determine if it is the intended recipient of the message [1]. If the device‘s assigned C-RNTI is in the control information message, the device processes that message [14]. The fact that a connected device in the cell receives multiple DCI messages is a point of vulnerability if an attacker can decode the messages and read the C-RNTI of other devices. Chapter 3 discusses an efficient method to decode the DCI messages. The method provides an attacker the ability to obtain a unique identifier for each device in the cell until assigned a new C-RNTI.

2.6.2 Subscription Permanent Identifier and Subscription Concealed Identifier

End users have to subscribe for the use of a particular 5G carrier, requiring each user device to have a permanent identifier. The permanent identifier is known as a SUPI or Subscription Permanent Identifier. It contains either an IMSI, a network-specific identifier (used on private networks), a Global Line Identifier (GLI), or a Global Cable Identifier (GCI) [15]. The GLI identifies a line connecting a Residential Gateway (RG) to the network. The GCI identifies a

cable that connects a RG to the network. Figure 2.15 displays the structure of a IMSI based SUPI. The Mobile Country Code (MCC) identifies the country the subscription is located [11, p. 20]. The Mobile Network Code (MNC) identifies the home Public Land Mobile Network (PLMN) for the subscription [11, p. 20]. The Mobile Subscriber Identification Number (MSIN) is a unique identifier for a subscription [11, p. 20].

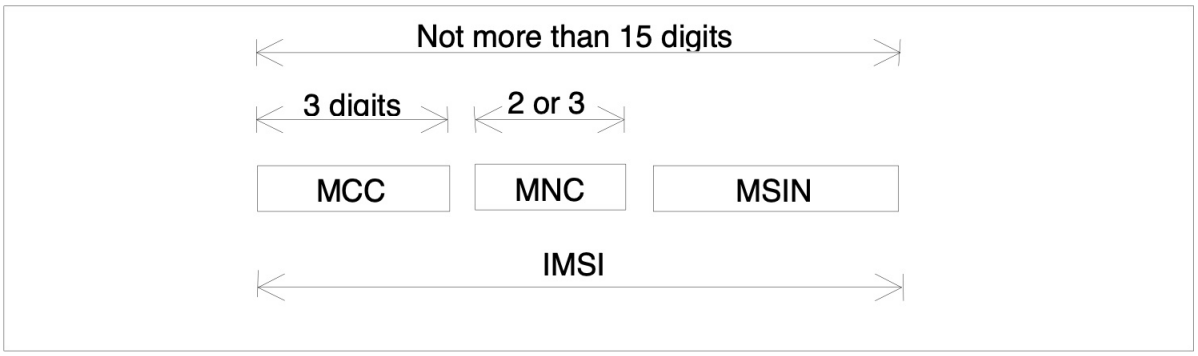

Figure 2.15. IMSI-based SUPI structure. Source: [11, p. 20].

The current 5G implementation reduces exposure of a SUPI by using two temporary identifiers in the authentication and registration setup. The two identifiers are the SUCI and 5G-GUTI. An UE conceals its SUPI within a SUCI. The SUCI contains the home network identifier and routing indicator in addition to the SUPI. The home network identifier and routing indicator allow the network to forward the SUCI to the AUSF of the home network. The home network retrieves the SUPI from the SUCI to authenticate the UE. The AMF assigns 5G-GUTI to user devices and this is unique to the device; however, it is also temporary [8, p. 97]. The 5G-GUTI contains two components that are the GUAMI and 5G-TMSI [11, p. 29]. The GUAMI contains the AMF identifier that assigned the 5G-GUTI [11, p. 29]. The 5G-TMSI identifies a piece of user equipment operating within the AMF [11, p. 29].

A few limited times, an UE transmits the SUPI without any protection or concealment. The first situation is when an UE needs to make an emergency call or is put into limited-service mode. In either of these situations, the user device‘s SUPI can be transmitted without

any concealment or encryption of the communication channel in order to connect to the gNB [10, p. 51].

2.7 Man-in-the-Middle Device

To conduct a MitM attack, an adversary requires a device capable of eavesdropping, injecting, and blocking communications between a base station and user equipment. The device must relay information between the two legitimate devices without being detected. The malicious device looks like a piece of user equipment to the base station and looks like a base station to the user equipment. In practice the device will act as a MitM between two legitimate parties‘ communication.

The adversary requires the device to first be able to relay and monitor traffic between the two legitimate devices. The malicious actor starts decoding DCI messages; this is done utilizing the work discussed in Section 3.1. Utilizing the C-RNTIs obtained from the DCI messages, the attacker can then impersonate a device to the legitimate base station and send messages to the user equipment acting as the base station.

2.8 Chapter Summary

This chapter introduced concepts of the different protocols and identifiers used in 5G. Vulnerabilities in the protocols will be discussed in Chapter 3. In addition, a way to decode DCI messages to obtain the C-RNTI will be discussed in the next Chapter. In Chapter 4, ways that an attacker can utilize and C-RNTI to target a single device will be explored.

CHAPTER 3:
Related Work

This chapter looks at work related to possible exploitation of user equipment on 5G by malicious actors. Section 3.1 demonstrates an efficient method that a passive observer can use to decode DCI messages to retrieve the C-RNTIs of the current set of user devices within the base station‘s range. Section 3.2 addresses potential vulnerabilities with the NAS and RRC protocols. Information from the related work gives a map on how an attack could be carried out and will be discussed further in Chapter 4.

3.1 Decoding of Downlink Control Information Messages

The Physical Downlink Control Channel (PDCCH) encodes the DCI messages to avoid passing identifiable information across the network between the base station and UEs, in addition to efficient addressing and error correction. The DCI message contains control information that is scrambled with the intended receiver‘s C-RNTI. Figure 3.1 shows the steps of the encoding process of the DCI messages. The process of encoding the message starts with computing the Cyclic Redundancy Check (CRC) for the message. The C-RNTI for the intended recipient is then added to the CRC and interleaved with the DCI message. The interleaving process results in each CRC bit placed behind the data that it is generated from [5]. Frozen bits are inserted in the message and then the message is polar encoded. The message then gets divided into 32 sub-blocks which are then interleaved. The message is then scrambled using a sequence generated by the C-RNTI of the assigned device. After the scrambling, the message is modulated for transmission [5].

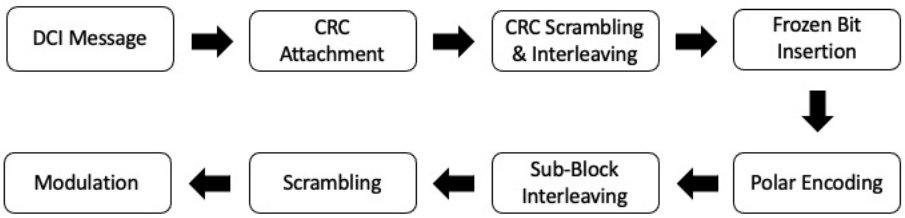

Figure 3.1. DCI message encoding sequence. Source: [1].

The reverse procedure is employed to decode the message. The message is demodulated and descrambled into logarithmic likelihood ratio (LLR) values. The LLR values are input for the polar decoder. The process uses a successive cancellation list (SCL) algorithm to decode the message into frozen bits and data. The frozen bits are in a fixed position and are forced to a value of zero during the process. The frozen bits are removed and the CRC is deleaved. The UE will decode these messages and, if the Radio Network Temporary Identifier (RNTI) matches the one assigned to the UE, it will continue to process the message. If an error is detected at any time in the process, the device moves to the next message and starts to decode that message. The decoding process is susceptible to a brute force method of decoding the data; however the attacker would have to try all the possible scrambling sequences [1].

Figure 3.2 sequences a method that allows a passive observer to recover the C-RNTIs from the PDCCH without having to try all possible scrambling sequences [1]. The method utilized in the recent research starts the process normally with the message being demodulated and deleaved into LLR values. The sub-blocks of LLR values are then passed through a decoding sequence that estimates the bit value. The parity of the bits is observed to determine which bits are the frozen bits. The main part of the method is the derivation of unique sequences of bits used to discover how the polar encoding changed particular bits during the encoding process [1]. A table of all possible unique sequences that are generated by a particular C-RNTI is developed. Comparing the frozen bits of the message with the table of unique sequences will provide the scrambling sequence. Using the scrambling sequence on the LLR sub-block values will reveal the C-RNTI of a device. [1]

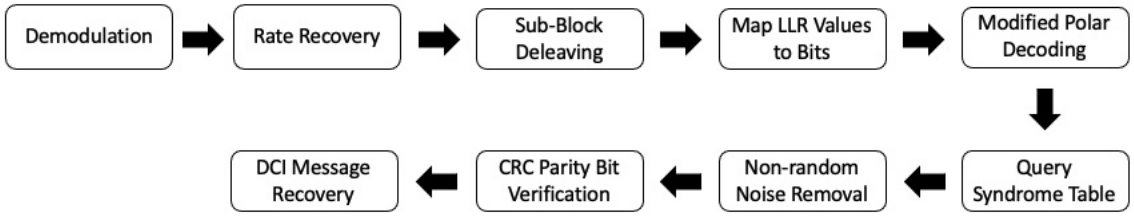

Figure 3.2. Method to decode DCI messages as a passive observer. Source: [16].

3.2 Protocol Vulnerabilities

Recent research studied the NAS and RRC layers and possible vulnerabilities associated with these layers [4]. The vulnerabilities allow various attacks to occur to include location tracking, discovering a SUPI, Denial-of-Service (DoS), battery draining, and downgrade. The vulnerabilities require knowledge of the C-RNTI assigned to a device and the ability to monitor and broadcast messages. The research assumed that the C-RNTI was known by the attacker but did not discuss how this could be achieved [4]. The attacks require a device with the capabilities to intercept, inject, forward, and block messages between a legitimate base station and the UE.

3.2.1 Non Access Stratum Layer

As previously discussed in Chapter 2, the NAS layer is responsible for the registration and authentication of a device on the network. The base station and UE complete these processes on the control plane. Research discovered vulnerabilities in the NAS layer that allowed location tracking, downgrade, and DoS attacks on the connected devices [4].

A vulnerability includes the handling of the sequence numbers that are used in verifying the messages. Both the UE and gNB use the NAS uplink sequence numbers to derive the K_{gNB} [8, p. 52]. If the numbers do not match during the key derivation process the two K_{gNB} will not match and secure communications cannot be established. The vulnerability requires that a rogue base station is able to monitor and broadcast messages. The adversary has to capture the `Security Mode Command` and `Security Mode Complete` messages during the initial registration. The messages contain a sequence number of zero. The messages are

held until the AMF sends another `Security Mode Command` message to refresh the keys used on the RRC layer. The attacker will then transmit the previously captured messages. The messages will pass verification because the overflow counter is still 0; however the AMF and UE update their local uplink and downlink counters, respectively. The attacker, at this point, has desynchronized the counters and forces the UE to start another registration procedure because the key used between the gNB and UE will not be correct. The attack can be repeated multiple times, denying the user device from establishing a new connection. Figure 3.3 depicts the sequence of this attack.

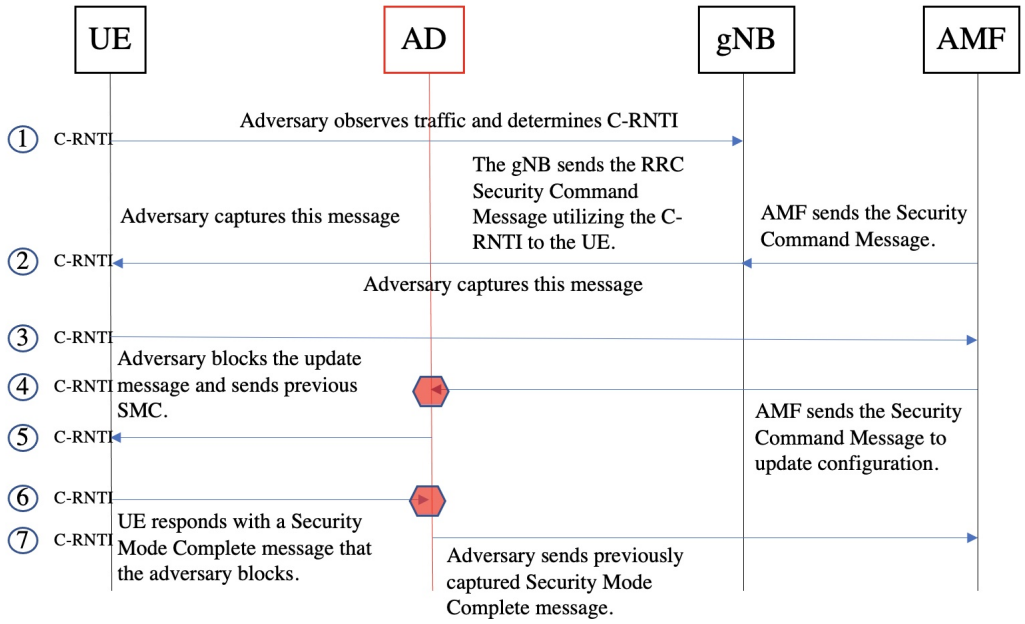

Figure 3.3. Diagram of an DoS attack in the NAS layer. Adapted from [4].

The attacker requires the C-RNTI of a device and ability to establish a device with MitM capabilities in order to conduct this attack. The MitM device must be able to intercept, forward, block, and inject messages into the normal traffic flow without being detected. The attacker then utilizes the device to send `Security Mode Command` messages with random MAC values to the UE. The device will decode the messages and sense the MAC value does not match what is expected, it will send a `Security Mode Reject` message to the AMF. Doing this repeatedly will desynchronize the NAS uplink counters. The AMF will discard

the uplink messages due to a mismatch between counters and it leads to a DoS attack on a particular device.

3.2.2 Radio Resource Control Layer

The RRC layer is responsible for establishing the connection between the gNB and the UE. The vulnerabilities are found in the setup and reconfiguration procedures. The attacks allow a malicious actor to conduct a DoS attack and expose the SUPI of a device. All the vulnerabilities in the RRC layer require knowledge of a device's C-RNTI.

3.2.3 Denial of Service Attack

An attacker can utilize the lack of integrity protection on the RRC Setup Request messages using a known C-RNTI [4].The lack of integrity protection allows the attacker to impersonate the target device during the setup request with the gNB. If integrity protection was enabled during this procedure, the attacker would have to break or find a way around the protection. For this attack, the attacker is impersonating the target UE after obtaining its C-RNTI. The random value in the `RRC Setup Request` message is the target's C-RNTI value. Since the values are reused, the base station will try to resolve this and could potentially delete the target device's security context, the agreed upon ciphering and integrity protection algorithms, forcing the target to reestablish that information. Without the security context the target will not have service until reestablished. Figure 3.4 illustrates the attack in the RRC layer.

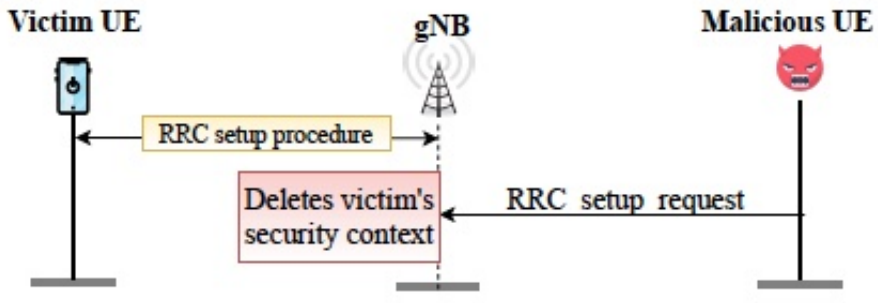

Figure 3.4. Diagram of an DoS attack in the RRC layer. Source: [4].

3.2.4 Exposing Permanent Identifier

An attacker can expose the SUPI by using the device's C-RNTI to send a `Security Mode Failure` message to the base station [4].The C-RNTI is unique to a device and used in the addressing of the messages. An attacker using a device's C-RNTI appears to be sending the message "on behalf" of the target.The technique involves observing the traffic and waiting for the gNB to send `Security Mode Command` message to the UE. The attacker sends a `Security Mode Failure` message to the base station. The attacker blocks the `Security Mode Complete` message from the UE. The UE and gNB did not complete the procedure for the security mode, leaving them using the previous configuration [10, p. 60]. If the previous configuration was null integrity and null ciphering protection (initial configuration), the device can be put into limited-service mode by sending the emergency registration request message [4]. An attacker requires that null integrity and null ciphering is used so that the attacker can utilize the `Identity Request` procedure in the next steps to reveal the SUPI. The attacker now sends a `Identity Request` message and the UE responds with `Identity Response` message containing its SUPI with no protection. Figure 3.5 illustrates the sequence of this attack.

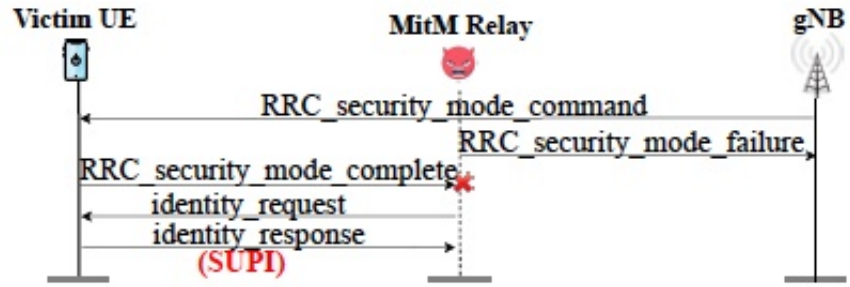

Figure 3.5. Diagram of attack revealing the SUPI of a user device. Source: [4].

3.3 Chapter Summary

The work presented in this chapter allows an attacker to label devices in the gNB cell. An attacker utilizes a fake base station to observe traffic within the cell and decode the DCI messages to get the C-RNTIs of the devices utilizing that base station. The C-RNTI of a

device is temporary, but using the vulnerabilities discovered in previous research allows an attacker to reveal the SUPI of a device to have a permanent identity for each device [4]. In addition to discovering the permanent identity, an attacker can conduct DoS attacks on the devices utilizing only their C-RNTI. The next chapter looks at the combination of both of these pieces of work to step through the process of the attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Attack Steps

This chapter synthesizes the previous work and lays out the steps necessary to conduct attacks on a 5G network. If an attacker wants to deny the use of the 5G network, destruction of the base station would achieve this goal. The attacker could jam the signals of the base station as well. These types of attacks are very noticeable and affect many pieces of equipment.

Sometimes attackers want to limit the visibility of their attack or target a particular device. To target a single device, it is required that the attacker discovers a label or identifier for the device. The ability for a passive observer to retrieve the C-RNTI from a DCI message, shown in Chapter 3, allows a temporary label to be assigned to a piece of user equipment. The adversary uses the C-RNTI to target a specific device to either conduct a Denial-of-Service attack or expose the SUPI. Specifically, the adversary uses the C-RNTI to ensure the messages go to the intended device or to block only those messages going to particular user equipment. By exposing the SUPI, the adversary obtains a permanent label for the user equipment. The attacks take place prior to the beginning of the ciphering of communication between devices and in some cases before integrity protection is used in the procedures that are vulnerable to misuse.

4.1 Vulnerable Procedures

The most vulnerable time to attack the phone is prior to the enabling of integrity protection and ciphering. The `RRC Setup` procedure takes place prior to the `Security Mode Command` procedure and the implementation of integrity protection and ciphering. The Security Mode Command procedure starts both integrity protection and ciphering as seen in Figure 4.1 [10, p. 59]. The UE starts integrity protection after the user equipment receives the `Security Mode Command` message from the base station [10, p. 60]. The `Security Mode Complete` message, sent from the UE, informs the base station of the successful start of integrity protection and ciphering on the user equipment; now all communication

between the two have both integrity protection and ciphering [10, p. 60]. In other words, attacks taking place prior to the `Security Mode Complete` message are easier to conduct.

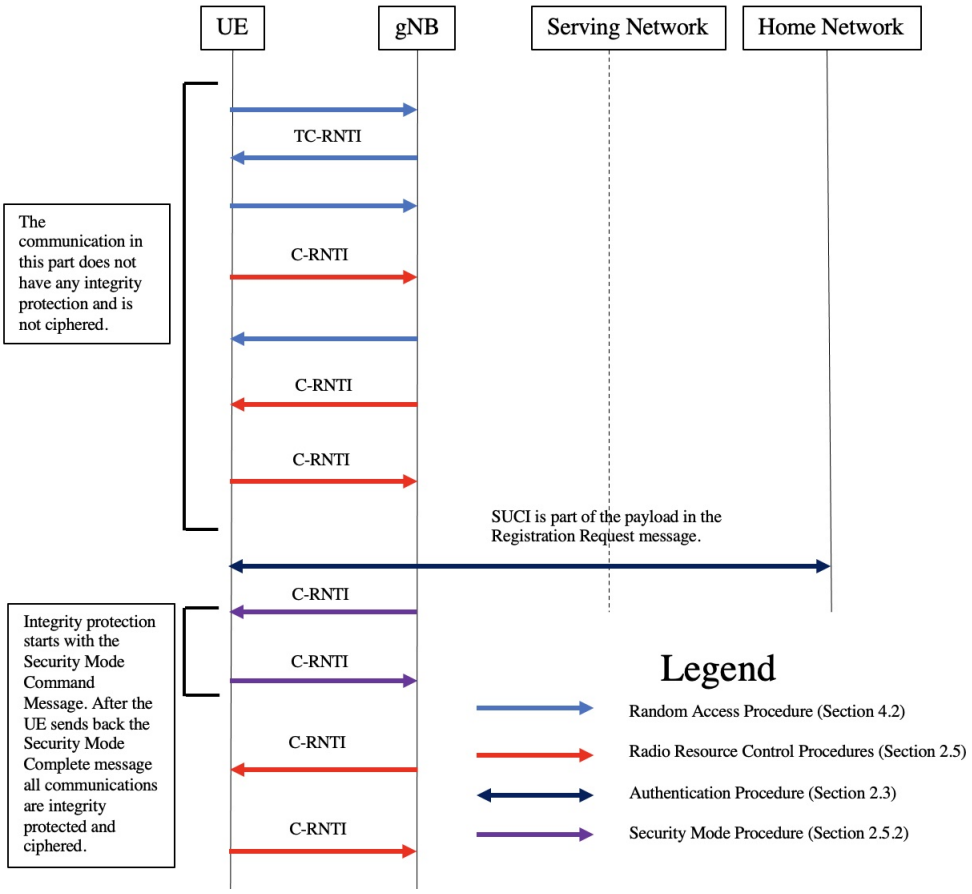

Figure 4.1. Flow of identifiers during initial setup of connection between gNB and UE.

Figure 4.1 shows the procedures between the UE and gNB leading up to the use of integrity protection and ciphering. The first procedure is the `Random Access Procedure`. The `Random Access Procedure` establishes the initial connection between the UE and gNB, and the assignment of a C-RNTI to the UE by the gNB. The second message contains a newly assigned Temporary Cell Radio Network Temporary Identifier (TC-RNTI). After the fourth message, the TC-RNTI becomes the device's C-RNTI if the value of the temporary

C-RNTI is not already assigned; if it is, the base station will assign a new C-RNTI. All communications between the gNB and UE can now be tracked using the C-RNTI to identify a piece of user equipment. After the establishment of the C-RNTI, the UE starts the Radio Resource Control Procedure.

The next procedure in the initial setup of the device with the gNB is the RRC setup and is discussed in detail in Chapter 2, Section 2.5.1. The RRC Setup Request message is sent to the higher layer as part of the payload of the last RAP message. This procedure is vulnerable to attack due to the lack of integrity protection and ciphering at this point. The following sections cover some of the methods of attack during this setup. The `RRC Setup Complete` message contains a dedicated NAS message that is the registration request for the core network. The registration request includes the user equipment's SUCI. The message does not have ciphering or integrity protection, so the SUCI is passed in the clear; however, the identity itself is an encrypted form of the SUPI [11, p. 21]. Figure 4.2 depicts the contents of the SUCI with the scheme output part containing the SUPI based on the algorithm being used [11, p. 21].

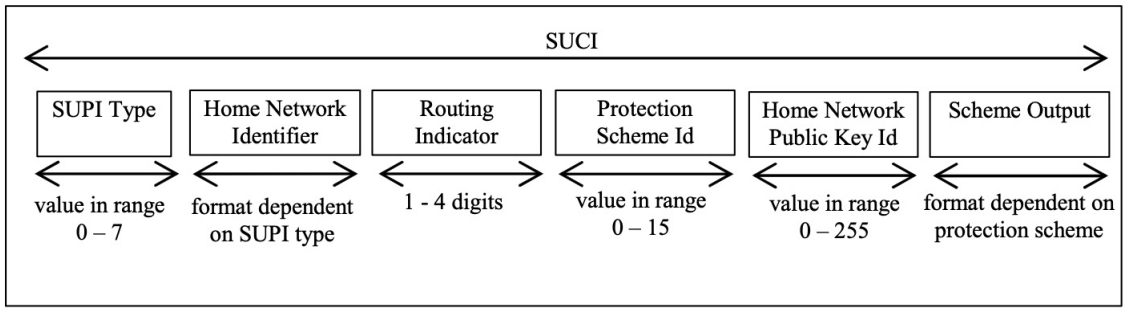

Figure 4.2. Subscription Concealed Identity contents. Source: [11, p. 21].

The registration request prompts the home network to authenticate itself and the device. Chapter 2 discusses the authentication process and includes a figure depicting the flow of the process. After the home network authenticates, the network sends the security context to the gNB. The base station starts the `Security Mode` procedure with the UE to establish which integrity and ciphering algorithms to use. The first message in this procedure, `Security`

`Mode Command`, is the start of the communications between the UE and gNB to include integrity protection [10, p. 59].

The lack of integrity protection and/or ciphering during initial setup provides an opportunity to an attacker to manipulate the communication between the user equipment and base station. The following sections describe the steps an attacker takes to affect the UE in different ways. At this point, the C-RNTI is the only label that we have been able to point to a device, and we use it in the following attacks to target a specific device. Since the C-RNTI is temporary, an attacker looks for a more permanent identifier to continue to identify a device across serving cells.

4.2 Exposing the Subscription Permanent Identifier

User equipment is uniquely identified through the SUPI by the network that provides services for that equipment. The role of the SUPI includes providing a permanent and unique identifier to the equipment for the network to validate that it is an authorized user and the authorized services that the device can utilize. The SUPI is discussed more in Section 2.6.2.

The SUPI allows an adversary to put a permanent label on a piece of user equipment, which could permit tracking of a device across multiple cells. The UE could move to another serving cell during this time and be assigned a new C-RNTI, forcing the attack all over. In other words, the major drawback for an attacker includes the repeated use of this attack to find the desired SUPI as the user equipment moves to new serving cells.

It may be possible to expose the SUPI on 5G networks. The attackers have to establish a device that can act as both a false base station and a piece of false user equipment. The device requires the capabilities to block or jam messages, inject messages into, and observe traffic on the network. The attack happens during the `Security Command Mode` procedure that is discussed in Section 2.5.2. The first step will be to observe the `Security Mode Command` message that is sent from the gNB to the UE to establish the security context, integrity protection, and ciphering algorithms. The attacker's device blocks the `Security Mode Complete` message from returning to the gNB when sent from the user equipment. The malicious device sends a `Security Mode Failure` message utilizing the C-RNTI of

the device. The gNB uses the previously established security context for communication. If the devices never established integrity protection and ciphering schemes, the null scheme is used for both integrity protection and ciphering.

The proposed scheme for exposing the SUPI is as follows: The adversary lets the initial `Security Command Mode` message through to the UE to finalize the initial registration and communication with the gNB. The message has integrity protection at this point and the UE is expecting that. The adversary sends the `Security Mode Failure` message, informing that it was not able to switch on the ciphering and integrity protection algorithms. This message can always be sent without ciphering or integrity protection [10, p. 909]. The failure message reverts to the previously used security configurations and keeps the UE in limited-service mode [8, p. 440]. At this point, the adversary sends the `Identity Request` message to get the SUPI in response.

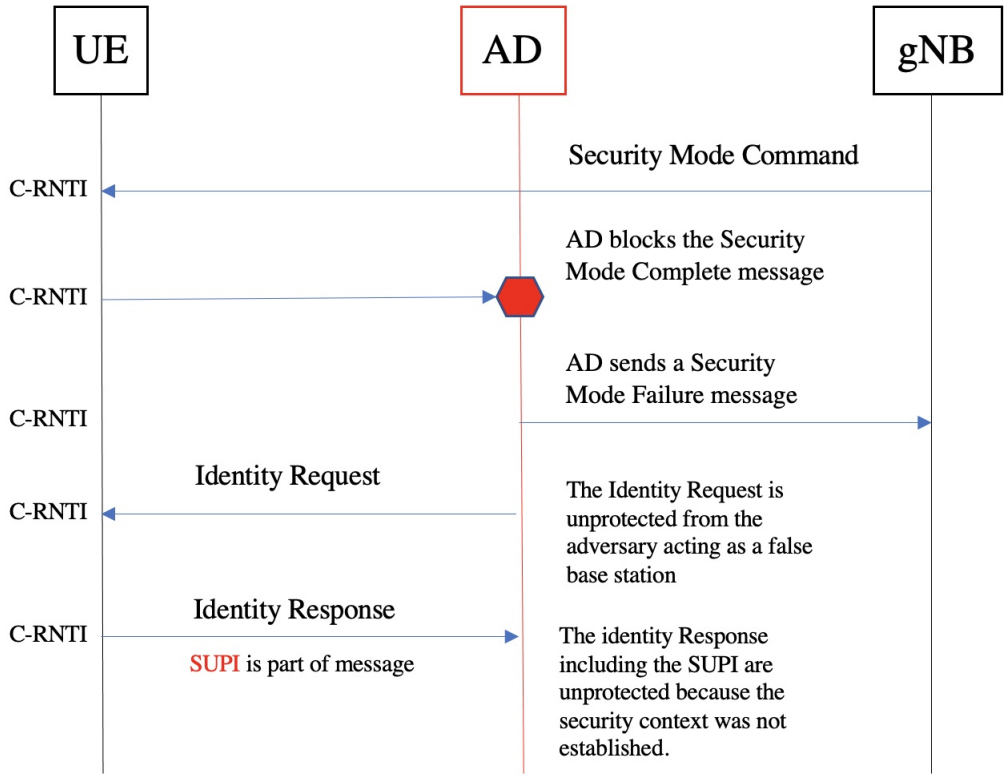

Figure 4.3. Exposing the SUPI after discovery of the C-RNTI.

The attacker does not require any knowledge of the integrity protection algorithm to conduct this attack. The attacker does require knowledge of a device's C-RNTI to target a device. The `Security Mode Failure` message is completely unprotected and sent without integrity protection or ciphering. The `Security Mode Failure` message is always sent without integrity protection and ciphering to inform the network that the security context, integrity protection and ciphering algorithms were not established on the UE. The network continues to use the previously established algorithms or the null-scheme algorithms. Using the null-scheme algorithms places the UE in a limited service mode. Once the UE and gNB are using the null-scheme, the adversary sends an `Identity Request` message to the UE. The user equipment responds with an `Identity Response` message containing the SUPI of the device. The messages are not protected because the base station and user equipment use the null-scheme for integrity protection and ciphering. Figure 4.4 shows the contacts of the SUCI with the null scheme [11, p. 22]. In other words, the SUCI now contains the unprotected SUPI.

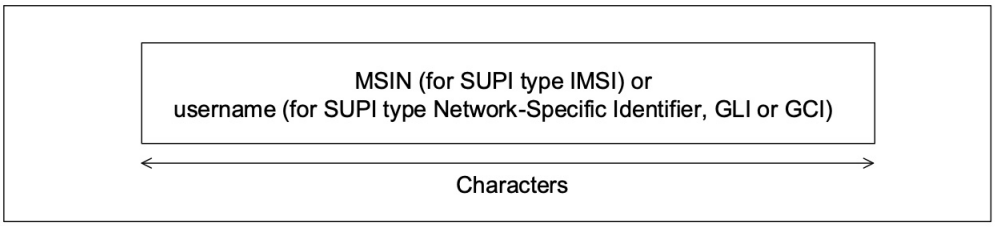

Figure 4.4. Null-scheme output of the SUCI. Source: [11, p. 22].

The implication of this attack is the ability to permanently identify a piece of user equipment. The attack will have to be repeated, though, as the equipment moves from one serving cell to another. The attack requires that each C-RNTI be identified, then the attack is executed. The process continues until the same SUPI is matched in order to re-identify an UE that has moved to a new cell.

A limitation of the attack is that it depends on whether the integrity protection and ciphering algorithms were already established. The limitation is caused because the network and UE just revert to using the previously established security algorithms; Figure 4.5 illustrates this case. In Figure 4.5, the null-scheme protection (S_0) is the default between the UE and gNB.

A security context (S_1) is successfully established prior to an adversary trying to conduct an attack to expose the SUPI. The adversary observes the network trying to establish a new security context (S_2) with the UE. The adversary attempts to expose the SUPI; however, the attack is unsuccessful. The UE and gNB continue with the previously established protections that provide full ciphering and integrity protection. Because previously established security context is used, the `Identity Request` and `Identify Response` messages used to obtain the SUPI, as seen in Figure 4.3, are both ciphered and have integrity protection. Based on the limitation, the only time to conduct this attack will be on the initial establishment of the integrity and protection algorithms, as seen in Figure 4.6. An example of when this could occur is the first time a phone is on a new network.

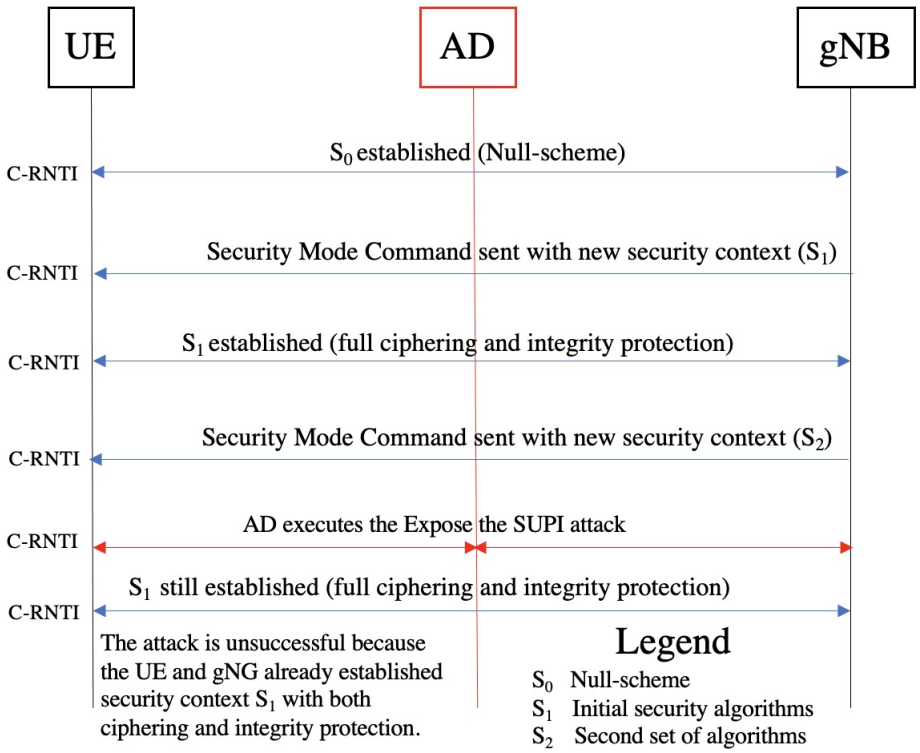

Figure 4.5. Unsuccessful attack to expose SUPI.

Due to the limitation, the adversary must conduct the attack at the initial establishment or break the establishment, as seen in Figure 4.6. The adversary interrupts the establishment

of the ciphering and integrity protection algorithms, forcing UE and gNB to use the null-scheme protection. The `Identity Request` and `Identity Response` messages are sent without any protection providing an un-ciphered SUPI, as explained in Section 4.2.

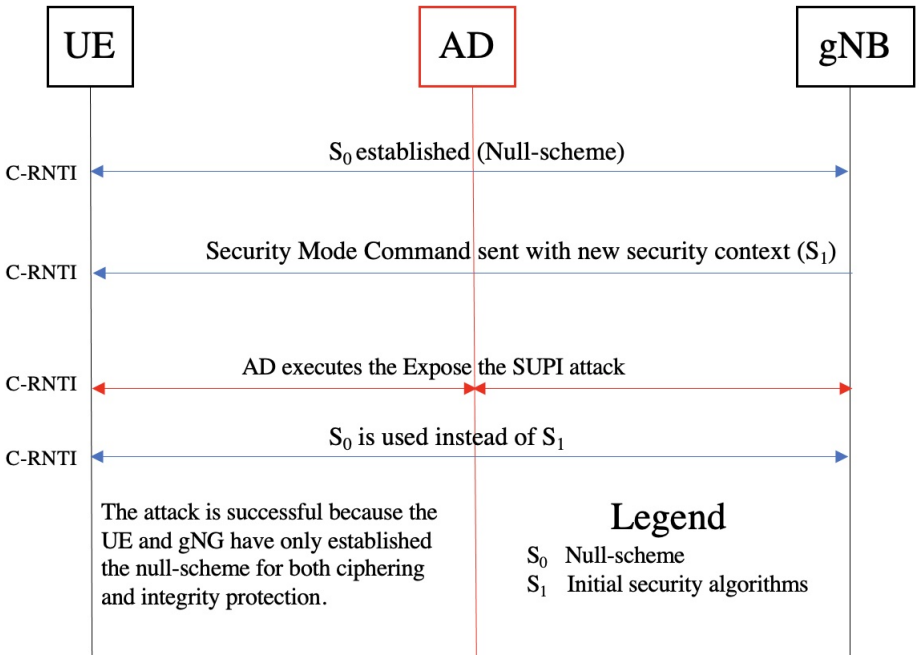

Figure 4.6. Successful attack to expose SUPI.

4.3 Radio Resource Control Denial-of-Service Attacks

All of the following attacks use the methodology discussed in Chapter 3, Section 3.2.2. The `RRC Setup` procedure contains different points that are susceptible to being interrupted and causing a Denial-of-Service between a UE and gNB. The adversary needs to have knowledge of the C-RNTI to target a single device.

4.3.1 Denial-of-Service 1

A malicious adversary first establishes a device that is able to observe the traffic between user devices and the gNB. Utilizing the methodology discussed in Chapter 3, the adversary

gains knowledge of C-RNTIs utilized in the serving cell. The second step in Figure 4.7 is the sending of an RRC Setup Request message created by the adversary with the target's C-RNTI. The third step involves the gNB dropping the original RRC connection context for the device associated with the C-RNTI used to create the setup request message.

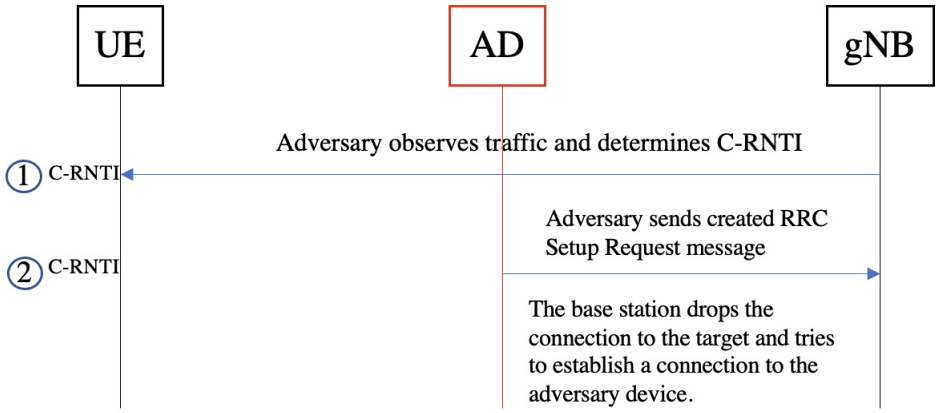

Figure 4.7. Denial-of-Service attack to disrupt the communication between the target and base station.

4.3.2 Denial-of-Service 2

An adversary observing traffic between user devices and the base station can decode the DCI messages' headers to obtain the devices' C-RNTIs. A second DoS attack occurs by the adversary disrupting RRC connection between the base station and the UE. The adversary uses the C-RNTI to send an `RRC Setup Reject` message to the UE. The user equipment sends an `RRC Setup Request` to the gNB. The adversary sends either `RRC Reject` or `RRC Release` messages to keep the target from establishing a connection. An `RRC Reject` message is sent from the gNB to reject or deny the `RRC Setup Request` message the user equipment sent. The `RRC Release` message is sent from the gNB to drop the RRC connection. Alternating the messages will avoid a time out condition [4]. Figure 4.8 depicts the steps in this attack.

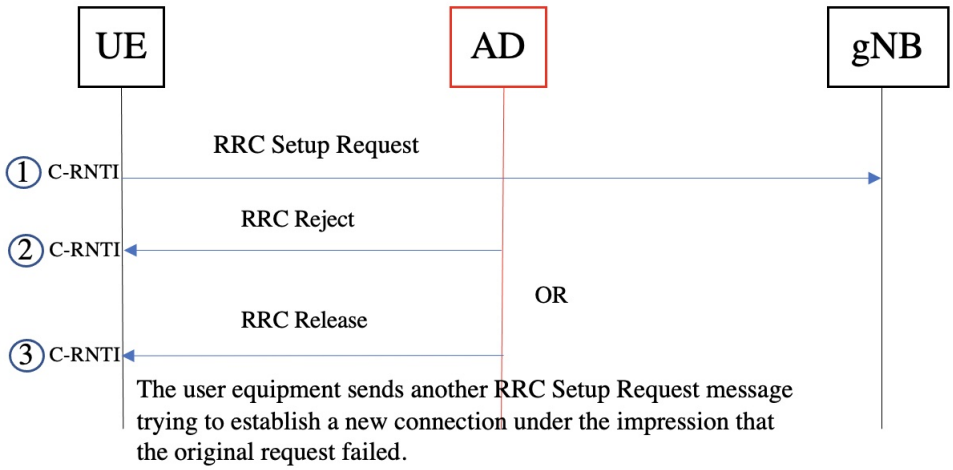

Figure 4.8. Denial-of-Service attack to disrupt the communication between the target and base station.

4.3.3 Denial-of-Service 3

The third DoS attack in the RRC procedure involves disrupting the RRC connection using the `RRC Reestablishment Request` and `RRC Reject` messages. This attack is very similar to the previous attack; however, the UE is in an `IDLE` state. The attacker starts with obtaining the C-RNTI of an user device. Using the C-RNTI, the attacker sends both the `RRC Reestablishment Request` and `RRC Reject` messages. The attacker alternates the sending of the two messages, denying the user device from establishing an RRC connection. The gNB sees this as a device that is not able to connect or fails for some unknown reason. The user equipment continues to try to reestablish connection but will eventually stop trying or find a different gNB to establish a connection. Figure 4.9 illustrates these steps.

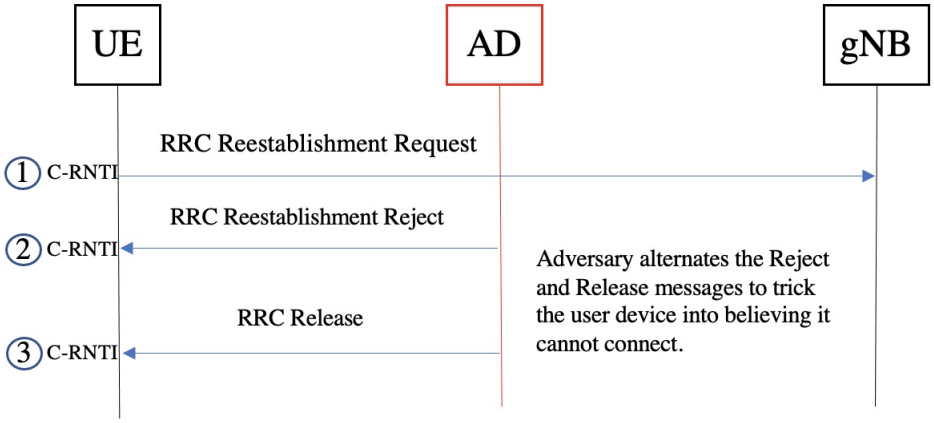

Figure 4.9. Denial-of-Service attack to disrupt the communication between the target and base station.

The attacks in this section affect the ability of the user equipment to connect to the base station. The UE will attempt to reconnect to the same gNB a few times. If the UE is not able to connect or reconnect to the same base station, it will attempt to see if another gNB is nearby and attempt to connect with that one. An attacker could use all three of the DoS attacks to prolong the amount of time that the UE is without service. Using a mix of the attacks would limit how fast the UE is looking for another base station by making it appear that it is able to connect and then severing the connection. These attacks could potentially be used to false user equipment to connect to false base stations.

4.4 Non-access Stratum Denial-of-Service

An adversary can cause a DoS attack by preventing the sequence numbers from matching during a `Security Mode Command` update message. If the sequence numbers do not match, the security mode reverts to the previous usable mode including the null protection scheme [8, p. 66]. The first step, as seen in Figure 4.10, involves the adversary monitoring traffic to capture C-RNTIs. After obtaining the C-RNTI, the adversary in the second step continues to monitor for the `Security Mode Command` message from the base station and captures this message to be replayed later in the attack. The UE sends a `Security Mode Complete` message back to the gNB; the adversary has to capture this message as well in step three of the attack. Step four is triggered when the adversary observes a new `Security`

`Command Mode` message. The adversary blocks this message from continuing to the UE. The adversary sends the previously captured `Security Command Mode` message in step five. The adversary blocks the `Security Command Complete` from the UE and sends the previously captured `Security Command Complete` message in steps six and seven.

The adversary uses the C-RNTIs to choose a device to affect with the DoS attack. The C-RNTI is not used to put together a message in this attack. Both the `Security Mode Command` and `Security Mode Complete` messages only have integrity protection [8, p. 66]. Using the previously captured messages throws off the sequence numbers used to produce the K_{gNB} [8, p. 48]. The rest of the keys used for ciphering between the user equipment and base station are derived from the K_{gNB}, as seen in Figure 2.2.

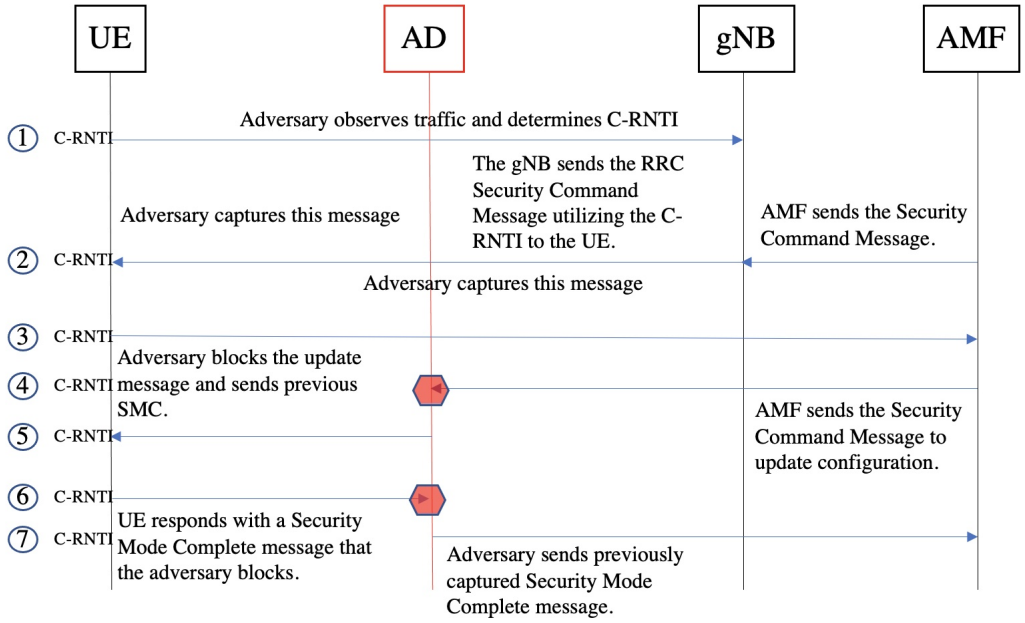

Figure 4.10. Denial-of-Service attack to disrupt the communication between the target and base station. Adapted from Source: [4].

The NAS Denial-of-Service attack disrupts the connection and authentication of a UE with the AMF. The user equipment will have to restart the authentication process again before

it will be reconnected fully. Repeated use of this attack along with the ones taking place in the RRC layer could make a DoS attack longer in duration.

4.5 Combining Attacks to Expose the Subscription Permanent Identifier

In Section 4.2, limitations to exposing the SUPI were discussed to include if the gNB and UE established security context prior to the attack. An adversary wants to have the UE revert back to the initial or default state prior to any type of security context being established. User equipment can be in one of three states with the network: idle (default), inactive, and connected [10, p. 50]. The connected and inactive states have security context established; however, when the UE is in the idle state, it releases the security context [10]. An adversary wants the device to return to the idle state if security context is already established in order to expose the SUPI.

The gNB utilizes the `RRC Release` message to put the UE into an idle or inactive state [10, p. 100], previously discussed in Section 2.5.1. The `RRC Release` message will be protected by both integrity protection and ciphering due to the previous establishment of both. The adversary will not be able to use the `RRC Release` message due to the protections. The adversary requires a method to get around the protection and return the UE to an idle state. A UE will revert to an idle state after a timeout period when the connection is lost [10, p. 104]. The timeout period varies and is determined by the network. The adversary will have to find a way to get the UE to timeout.

A possible way an adversary gets the UE back into the idle state is by conducting a DoS attack on a specific UE utilizing its C-RNTI. DoS attacks in Sections 4.3 and 4.4 illustrated ways to conduct the attacks. Figure 4.11 illustrates the adversary's use of DoS attacks to force the UE back to the idle (default) state. Once the UE is back in the idle state, the adversary conducts an attack to expose the SUPI.

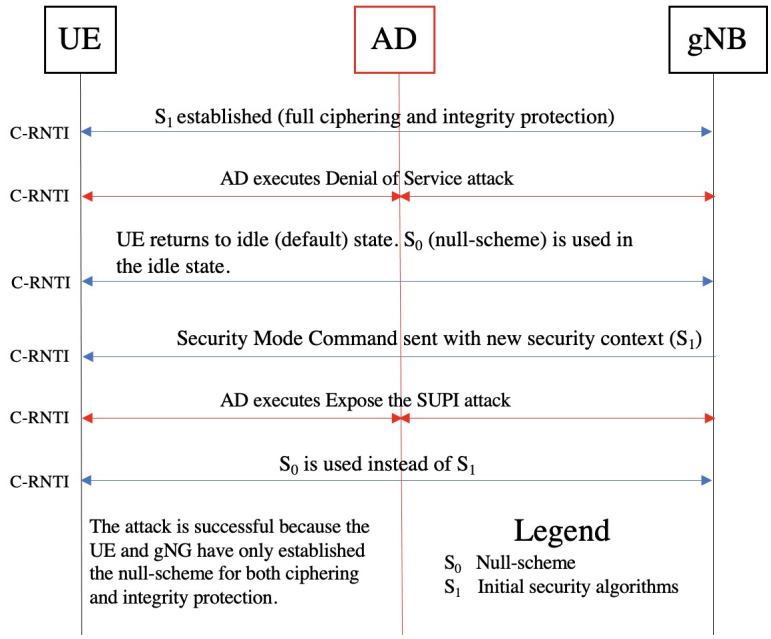

Figure 4.11. Combined DoS and Expose the SUPI attack.

4.6 Proposed Methodology of Tracking a Piece of User Equipment

The SUPI and C-RNTI scope of traceability is limited. The C-RNTI's scope provides traceability only within a serving cell, providing a local scope. The adversary cannot rely on the C-RNTI transferring to a new serving cell. The scope of the SUPI is global and permanent, but, the adversary will need to expose the SUPI to track the UE between different gNBs. Tracing the SUPI involves exposing the identifier each time that the device travels to a new serving cell. This requires the adversary to obtain the C-RNTIs and expose the SUPI for each UE in a serving cell until the matching SUPI is found. Table 4.1 summarizes the scope and use of each identifier.

Identifier	Scope	Assigned to	Assigned by	Use
C-RNTI	Local	UE	gNB	Temporarily identifies an UE in the serving cell, ensuring that UE receives only the messages it is supposed to receive.
SUPI	Global	UE	Home Network	Permanently identifies a network subscriber (UE) with a unique label.

Table 4.1. Summarizes the C-RNTI and SUPI scope and use.

4.6.1 Step 1—Set Up an Observation Post

First, an adversary has to establish is an observation post. The adversary needs to be able to observe communications between a base station and user equipment. After observing and recording the communications, an adversary can go to the next step and start decoding messages. This step allows an adversary to move to the next step to decode the DCI messages to obtain the C-RNTI. It would be most efficient to have an observation post set up prior to communications from the UE an adversary wants to track. Figure 4.12 depicts this step.

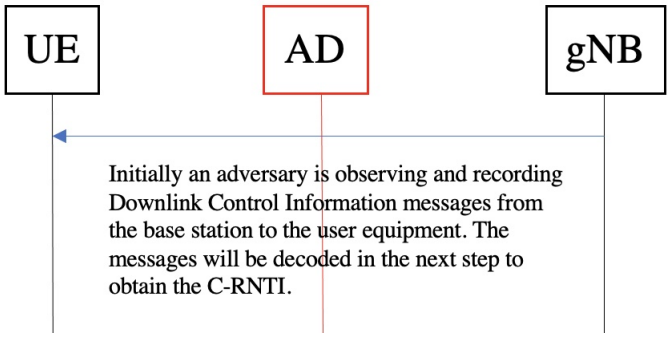

Figure 4.12. Adversary observes DCI messages in initial step of the attack.

4.6.2 Step 2—Decode Messages

The second step includes the decoding of DCI messages. The DCI messages contain the C-RNTI to ensure that the message is delivered to the intended recipient. At this time, the adversary utilizes the method discussed in Section 3.1 to obtain the C-RNTI of a UE and the scrambling sequence used in the modulation of the DCI message [1]. The attacker now possesses a temporary label, the C-RNTI, and the scrambling sequence used in sending DCI messages to a specific device [1].

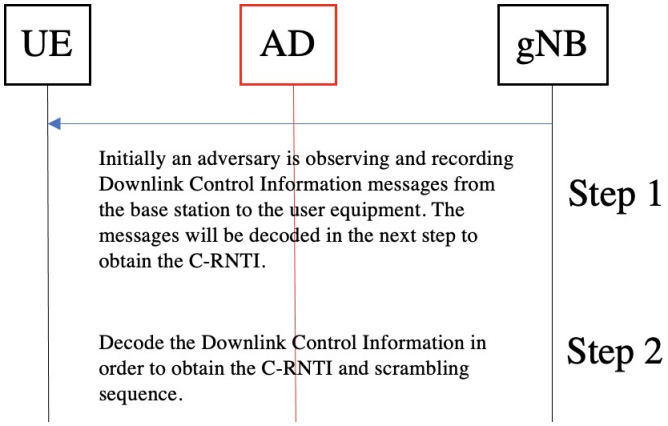

Figure 4.13. Adversary decodes DCI messages in second step of the attack.

With a C-RNTI, an adversary can trace a piece of user equipment while that UE remains in the serving cell. The UE can be assigned a new C-RNTI when moving between serving cells, if the base station refreshes the connection, and if the UE goes from active to idle to active [10]. The adversary may attempt to get a permanent identifier for the UE and that includes the SUPI. The permanent identifier allows an adversary to track the device between base stations.

4.6.3 Step 3—Expose Permanent Identity

Traceability of a UE requires the capture of the SUPI due to the fact that the SUPI is the permanent identifier used to authenticate the UE as discussed in Section 2.6.2. The 5G network introduced additional security mechanisms to prevent the SUPI from being passed

in the clear. A possible method to discover or expose the SUPI was discussed previously in the chapter in Section 4.2. Once an attacker has the SUPI, he possesses a permanent identifier for user equipment.

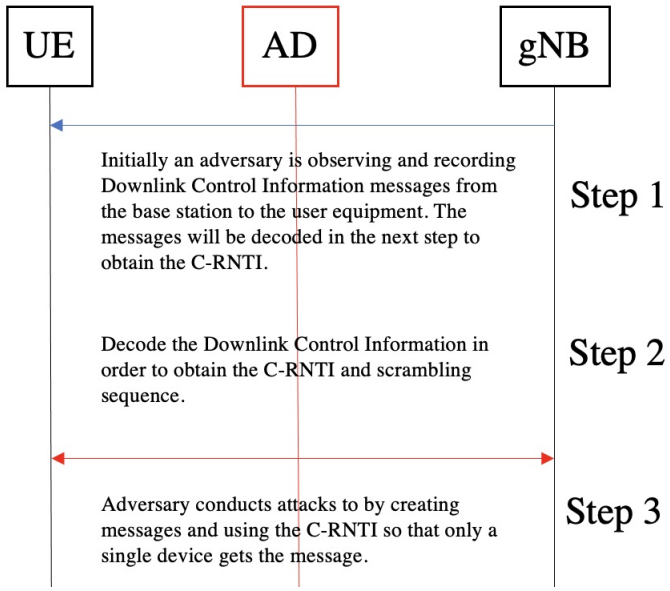

Figure 4.14. Adversary conducts attacks in third step of the attack.

The adversary obtains a permanent identification for a piece of user equipment after obtaining the SUPI. A limitation for the adversary is that every time the UE obtains a new C-RNTI, the SUPI will have to be exposed again. The exposure allows an adversary to ensure that the same device is being tracked.

4.6.4 Step 4—Other Attacks

An adversary in this step can carry out one of the other attacks discussed in this chapter in Sections 4.3 and 4.4. The attacks are DoS actions and can be carried out prior to exposing the SUPI for a device. However, carrying out the attacks utilizing the C-RNTI without exposing the SUPI could cause the adversary to affect unintended targets.

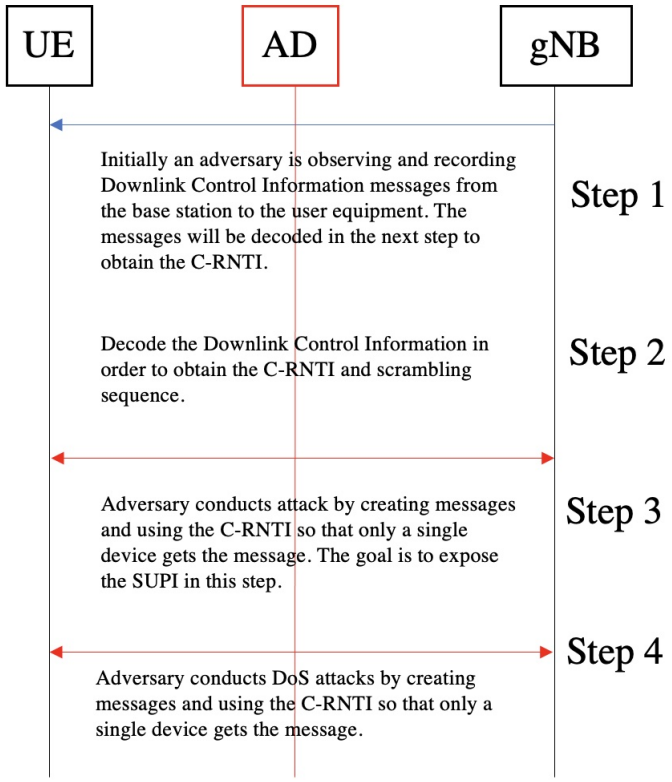

Figure 4.15. Adversary conducts attacks in fourth step of the attack.

4.6.5 Step 5—Repeat

An adversary continues with this series of steps for long-term tracking of a piece of user equipment. This is because the SUPI has to be exposed each time to verify that device is still within the serving cell. The temporary identity, C-RNTI, is easily obtained through passive listening and decoding of DCI messages. Since the gNB reuses C-RNTIs, an adversary should check that the SUPI is still the same.

4.6.6 Limitations

The biggest limitation to tracking a UE with just a C-RNTI is the temporary nature of this identifier. An adversary requires the C-RNTI to send messages impersonating a UE. As previously discussed in Section 2.6.1, C-RNTIs are the mechanism that ensures only the intended recipient receives its traffic and the gNB knows who sent the messages. Since

C-RNTIs don't migrate from one serving cell to the next; an adversary needs a permanent identifier, the SUPI, to verify that the same device is now in a new serving cell. The SUPI, as discussed in Section 2.6.2, is a unique identifier that is permanently assigned to the UE.

C-RNTIs change periodically for several reasons. The biggest reason is when changing serving cells; however, the C-RNTI sometimes change within the same serving cell either because it was refreshed by the gNB, the device disconnects and then reconnects, or it goes to an idle state. Section 2.6.1 discussed the assignment of an I-RNTI when a device goes idle. Due to the temporary and changing nature of a C-RNTI, an adversary will need to check the SUPI to ensure that the same device is being tracked. The SUPI will need to be exposed every time that a phone changes serving cells and periodically while still in the same cell. If an adversary does not verify that the SUPI is still the same, the C-RNTI used on a device could change without the adversary being aware. The C-RNTI gets reassigned as devices move in and out of the serving cell of the gNB hence requiring a periodic exposure of the SUPI to verify the UE is still the same.

The rechecking of the SUPI will require that the adversary obtains C-RNTIs currently in use and start running through the steps to expose the SUPI. Exposure of the SUPI further allows an adversary to match with a SUPI of the tracked device. If the adversary is not able to match a SUPI before the device goes idle or moves to a different serving cell, there will not be a way to ensure that device was ever in the serving cell by the C-RNTI alone.

Ultimately, the difficulty of exposing the SUPI may want to track a device only for the time it is in a serving cell. For example, an adversary may want to deny a portion of the devices in serving cell. The adversary would not need to expose the SUPI to track the device; however, the adversary would still need to capture the C-RNTIs to conduct the DoS attacks discussed in Sections 4.3 and 4.4.

4.7 Chapter Summary

The attacks described in this chapter take place before ciphering and in some cases prior to both integrity protection and ciphering. All the attacks utilized the C-RNTI to label or temporarily identify a piece of user equipment prior to attack. One attack in particular discusses a way to expose the SUPI for permanent identification of a UE that would allow

persistent targeting. Further work needs to be done to see how these attacks affect the network patterns, behavior of devices, and practicable application of the attacks. Understanding this information and how the attacks are carried out will lead to better defenses and security implementations.

CHAPTER 5:
Conclusion and Future Work

Chapter 5 summarizes the previous chapters and recommends future work that is related.

5.1 Conclusion

This thesis studied the different ways that a exposed C-RNTI can be used to attack a 5G device. Researchers examined different protocols and concluded that if the attacker knew the C-RNTI it would be possible to attack a the device with that assigned C-RNTI. The attacks included several different DoS attacks, exposing the SUPI, and preventing the device from getting a new C-RNTI.

Chapter 2 provided an overview of 5G and some detail about parts of the implementation of 5G. In particular, identifiers (C-RNTI, SUPI, SUCI) were discussed to provide some information on how they are used and when they are assigned. Additionally, detail about procedures vulnerable to an attack were discussed.

Chapter 3 described vulnerabilities in procedures that happen prior to integrity protection and ciphering. The vulnerabilities allow possible attacks to include Denial of Service, location tracking, and exposure of the SUPI. The chapter discusses a method on decoding DCI messages to obtain a C-RNTI. Knowledge of the C-RNTI allows targeting of a single device within the serving cell.

Chapter 4 pulled together the various pieces of research and depicted the steps necessary to conduct one of the previously mentioned attacks. The general steps are to establish a False Base Station (FBS), obtain the C-RNTI, and then conduct the attack. The attacker may repeat attacks to produce another effect to further gain information about a device. The C-RNTI must be obtained prior to these attacks and in order for that happen, the attacker will need to set up a False Base Station to collect DCI messages. Combining the discovered C-RNTI with attacks discussed in Chapter 3 allows an attacker to target a specific device. The thesis also explored ways to obtain a C-RNTI then conduct DoS attacks to observe behavioral pattern changes of devices in a serving cell.

5.2 Future Work

Future work in this area includes simulating the attacks, developing defensive measures, and looking at how the Integrated Access and Backhaul capability can be combined with these attacks.

5.2.1 Attack Simulations

Simulations of the attacks described in this thesis provides information on the behavior of the attack and difficulty in conducting the attack. From analysis of that information both changes to current implementations, possible defenses, and network patterns to detect the attack are possible outcomes of that research.

5.2.2 Integrated Access and Backhaul

Integrated Access and Backhaul (IAB) technology allows some user equipment to act as a relay. The backhaul portion of the network is the part that connects the core network to the base stations. The IAB further extends the access and core network functions to nodes further down the chain. Analysis of the creation and protection of these nodes is important to understand as they could potentially provide an additional point of access to a network for malicious actors.

List of References

[1] B. Gardner and J. Roth, "An efficient methodology to de-anonymize the 5G-new radio physical downlink control channel," in *ICASSP 2020—2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, May 2020.

[2] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.

[3] N. Kshetri and J. Voas, "5G, security, and you," *Computer*, vol. 53, no. 3, pp. 62–66, Mar. 2020.

[4] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5GReasoner," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Nov. 2019.

[5] E. Dahlman, *5G NR : The Next Generation Wireless Access Technology*. London, UK: Academic Press, 2018.

[6] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[7] O. Hanane and M. Tomader, "4G and 5G," in *Proceedings of the 4th International Conference on Big Data and Internet of Things*. ACM, Oct. 2019.

[8] 3GPP, "Security architecture and procedures for 5G system," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 33.501, Apr. 2021, version 17.1.0. Available: http://www.3gpp.org/DynaReport/33501.htm

[9] 3GPP, "NR; NR and NG-RAN Overall description; Stage-2," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.300, Mar. 2021, version 16.5.0. Available: http://www.3gpp.org/DynaReport/38300.htm

[10] 3GPP, "NR; Radio Resource Control (RRC); Protocol specification," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.331, Mar. 2021, version 16.4.1. Available: http://www.3gpp.org/DynaReport/38331.htm

[11] 3GPP, "Numbering, addressing and identification," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.003, Mar. 2021, version 17.1.0. Available: http://www.3gpp.org/DynaReport/23003.htm

[12] J. H. Bae, A. Abotabl, H.-P. Lin, K.-B. Song, and J. Lee, "An overview of channel coding for 5G NR cellular communications," *APSIPA Transactions on Signal and Information Processing*, vol. 8, 2019.

[13] C.-C. Tseng, L.-H. Wang, F.-C. Kuo, and H.-C. Wang, "The design of low-latency random access procedure for 5G," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, June 2020.

[14] 3GPP, "NR; Multiplexing and channel coding," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.212, Mar. 2021, version 16.5.0. Available: http://www.3gpp.org/DynaReport/38212.htm

[15] 3GPP, "System architecture for the 5G system (5GS)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.501, Mar. 2021, version 17.0.0. Available: http://www.3gpp.org/DynaReport/23501.htm

[16] B. Gardner, "An efficient methodology to de-anonymize the 5G-new radio physical downlink control channel," Master's thesis, Naval Postgraduate School, 2020, includes supplementary material. Available: http://hdl.handle.net/10945/65524

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California