Computing (2021) 103:425–447
https://doi.org/10.1007/s00607-020-00855-0

SPECIAL ISSUE ARTICLE

Towards 5G-based IoT security analysis against Vo5G eavesdropping

Sungmoon Kwon[1] · Seongmin Park[1] · HyungJin Cho[1] · Youngkwon Park[1] · Dowon Kim[1] · Kangbin Yim[2]

Received: 15 September 2020 / Accepted: 13 October 2020 / Published online: 3 January 2021

Abstract
With the advent of 5G technology, the enhanced Mobile Broadband technology is translating 5G-based Internet of Things (IoT) such as smart home/building into reality. With such advances, security must mitigate greater risks associated with faster and more accessible technology. The 5G-based IoT security analysis is crucial to IoT Technology, which will eventually expand extensively into massive machine-type communications and Ultra-Reliable Low Latency Communications. This paper analyses the countermeasures and verification methods of eavesdropping vulnerabilities within IoT devices that use the current 5G Non-Standalone (NSA) network system. The network hierarchical structure of 5G-based IoT was evaluated for vulnerability analysis, performed separately for 5G Access Stratum (AS), Non-Access Stratum (NAS), and Internet Protocol (IP) Multimedia Subsystem (IMS). AS keystream reuse, NAS null-ciphering, and IMS IPsec off vulnerabilities were tested on mobile carrier networks to validate it on the 5G NSA network as well. A countermeasure against each vulnerability was presented, and our Intrusion Detection System based on these countermeasures successfully detected the presented controlled attacks.

✉ Kangbin Yim
yim@sch.ac.kr

Sungmoon Kwon
skwon@kisa.or.kr

Seongmin Park
smpark@kisa.or.kr

HyungJin Cho
hjcho86@kisa.or.kr

Youngkwon Park
young6875@kisa.or.kf

Dowon Kim
kimdw@kisa.or.kr

[1] Korea Internet Security Agency, Naju, Korea

[2] Department of Information Security Engineering, Soonchunhyang University, Asan, Korea

Keywords IoT · 5G · Eavesdropping · Vo5G · 5G NSA · 5G security · IDS

Mathematics Subject Classification 68M25

1 Introduction

With the introduction of 5G, the enhanced Mobile Broadband (eMBB) technology is transforming 5G-based Internet of Things (IoT) such as smart home and smart building into reality. In 2020, it is estimated that 20 billion IoT devices are connected to the Internet [1], and as of 2019, 80,000 5G base stations [2] are installed in South Korea, 130,000 5G base stations [3] in China, and hundreds of thousands of 5G base stations are operational around the globe. The 5G Non-Standalone (NSA) network is now commercialized around the world and has enabled the enhanced Mobile Broadband (eMBB) technology. The 5G Standalone (SA) network was launched in the US, China, initially, and has evolved ever since for IoT to be more widespread with the introduction of the massive Machine Type Communications (mMTC) and Ultra-Reliable Low Latency Communications (URLLC) technology. As IoT devices incorporate 5G network, it leads to the development of industries such as the smart home of eMBB but at heightened security risks. If IoT devices with insufficient security design are connected to the 5G network, it may lead to eavesdropping and charge avoidance due to the vulnerabilities of the devices. Accordingly, in line with the age of 5G-based IoT, analysis of vulnerabilities and IoT device design, which supplement these vulnerabilities, are necessary.

This paper describes the security analysis against eavesdropping of users' calls likely to occur in the case of eMBB smart homes. As the 5G NSA network is using the 4G LTE core network, whether or not the vulnerabilities of 4G LTE are valid for the 5G NSA remains in question. Through the experiments of this study, it was confirmed that the vulnerabilities, i.e. Access Stratum (AS) keystream reuse [4], Non-Access Stratum (NSA) null-ciphering [5] and Internet Protocol (IP) Multimedia Subscriber (IMS) IP security (IPsec) off [6] are valid for the 5G NSA mobile carrier networks. Accordingly, this paper presents effective countermeasures against vulnerabilities of the 5G NSA network and describes the details of verifying them.

This paper has the following composition. Section 2 describes the structure of 5G NSA and security as background, and Sect. 3 describes works related to 5G security. Sect. 4 describes the vulnerabilities of the 5G-based IoT system, and Sect. 5 presents countermeasures against the vulnerabilities in Sect. 4. Section 6 describes attack scenarios using vulnerabilities, results of attack experiments, and the Intrusion Detection System (IDS) for detection and results. Finally, Sect. 7 concludes the paper.

2 Background

The Third Generation Partnership Project (3GPP) is a joint research project among organizations related to mobile communication. It writes the standards for 5G systems. Looking at the structure of 5G, some SAs implemented the 5G core network without using NSA and LTE, which use the existing 4G LTE network. 5G SA is still in its infancy, and as exploit and countermeasure experiment are difficult, the scope of this paper is limited to 5G NSA.

2.1 5G Non-Standalone (NSA) architecture

5G NSA is using the existing 4G LTE network as the core network. The biggest difference from existing 4G LTE is the use of next-generation Node B (gNB) for 5G service. gNB transmits User Equipment (UE) data, and eNB controls UE. Figure 1 is a simplified 5G NSA structure diagram of the configuration of the components necessary for this paper. Each component of 5G NSA is described below.

User Equipment (UE) UE means the user terminal, and includes a smartphone, a USB modem, a computer with a built-in mobile communication module, and smart home IoT, which is one of the key services of eMBB.

evolved Node B (eNB) It provides wireless interface to UE, and in 5G it is used for functions related to UE control.

next generation Node B (gNB) It provides wireless interface to UE, and it is used for data transmission.

Mobility Management Entity (MME) MME manages UE authentication and connection state and activation state.

Home Subscriber Server (HSS) HSS is a central database that manages the key information and subscriber profile for authentication of each UE. When UE connects to network, it delivers the key information and subscriber profile for UE authentication to MME.

Serving Gateway(S-GW) S-GW routes and delivers user packets between base stations and P-GW, and when UE performs hangover between eNB and gNB, it serves as the anchoring point.

Packet data network Gateway (P-GW) P-GW connects UE to the external Packet Data Network (PDN). It serves as a path for delivering packets between UE and PDN, and performs such function as charging according to data use and allocation of the Internet Protocol (IP) addresses of UE.

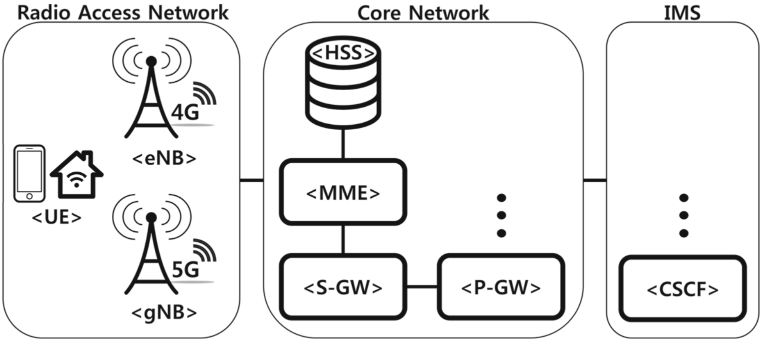


Fig. 1 5G NSA architecture

Call Session Control Function (CSCF) CSCF is a component of the IP Multimedia Subsystem (IMS), which is one of the PDNs and provides voice calling service. It processes the Session Initiation Protocol (SIP) [7] signaling packets of IMS.

The uplink data of Vo5G is transmitted along the UE—gNB—S-GW—P-GW—CSCF path, and the downlink data is transmitted along the reverse path. If two UEs use Vo5G through different mobile carriers, the process of transmitting data to the other party's IMS is added.

2.2 5G Non-Standalone (NSA) security

As all UEs are controlled through eNB, the security setting process is the same as in existing 4G LTE. In LTE, UE management is divided into Access Stratum (AS) and Non-Access Stratum (NAS). AS covers management of UE, eNB and gNB on the Radio Access Network (RAN). NAS manages connection through communication between UE and the MME of the core network. Besides, it supports the Internet Protocol Security (IPsec) between PDN and UE, and in IMS PDN, CSCF performs the role of the Security Gateway (SEG) for communication between UE and IPsec. Accordingly, AS/NAS security process and IPsec will be described as security for 5G SNA.

2.2.1 Access Stratum (AS)/Non-access Stratum (NAS) security process

The AS/NAS security process is conducted in the order of mutual communication between UE and the core network, NAS security setup and AS security setup. Figure 2 shows the sequence diagram of the AS/NAS security procedure. In the authentication

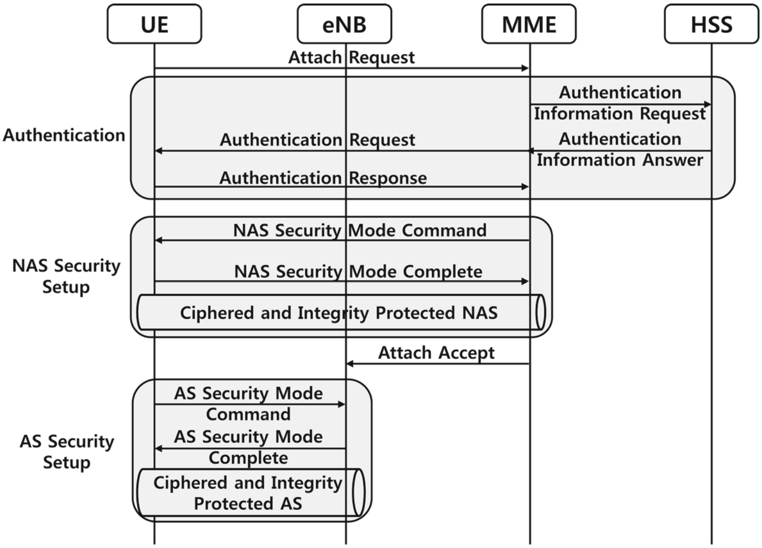

UE
eNB
MME
HSS
Attach Request
Authentication
Authentication Information Request
Authentication Request
Authentication Information Answer
Authentication Response
NAS Security Setup
NAS Security Mode Command
NAS Security Mode Complete
Ciphered and Integrity Protected NAS
Attach Accept
AS Security Setup
AS Security Mode Command
AS Security Mode Complete
Ciphered and Integrity Protected AS

Fig. 2 Sequence diagram of AS/NAS Security procedure

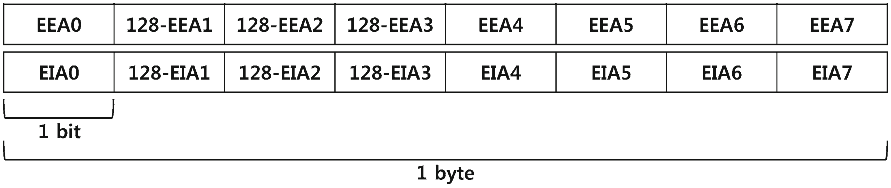
stage, UE and MME performs mutual authentication through the Evolved Packet System Authentication and Key Agreement (EPS AKA) procedure. UE transmits the supported encryption and integrity verification option (UE network capability), the International Mobile Subscriber Identity (IMSI), i.e. the unique ID of the device, etc. as an Attach Request message to request authentication. MME saves UE security capability and request HSS for user authentication. HSS transmits authentication vectors for identifying and authenticating users to MME, and MME picks vectors from the authentication vectors, transmits them to UE and performs authentication. The authentication result shows that UE and MME shares the key, and generates NAS and AS from this key.

In the NAS security setup stage, security setup of UE and MME is performed. MME sets the encryption and integrity option, and transmits the NAS Security Mode Command message, including UE network capability received during authentication. UE compares the UE network capability it transmitted and the received replayed UE network capability, and if the two values are different, it must be able to deny session connection. If UE network capability is normal, it completes NAS security setup by transmitting the Message Authentication Code (MAC) as a message including the received NAS Security Mode Command message and key.

In the AS security setup stage, security setup of UE and eNB is performed. eNB receives the UE network capability that MME received in the Authentication stage, and performs AS security setup based on this. Other procedures are similar to the NAS security setup procedure except that the subject is changed from MME to eNB.

If UE and eNB are connected, UE starts measurement of 5G New Radio (NR). UE receives the primary/secondary synchronization signal from gNB, performs synchronization, and reports 5G signal quality to eNB. In reference to the quality of the 5G signal received from UE, eNB checks the throughput requirements of the 5G connection between UE and gNB and 5G coverage. If 5G connection is deemed to be appropriate, eNB transmits communication settings, including UE capabilities and security information, to gNB. Accordingly, there is no separate security process for connection between UE and gNB, and the security settings between UE and eNB will be used as is. Then, after the connection reconfiguration, copying data from eNB to gNB and path update stage for communication between UE and gNB, it performs 5G communication.

Figure 3 shows field of UE network capability. The encryption and authentication field comprises the 1-byte EPS Encryption Algorithm (EEA) and the 1-byte EPS Integrity Algorithm (EIA). EEA0 and EIA0 mean cases where no algorithm is used at all. 128-EEA1 and 128-EIA1 mean the 128 bit SNOW 3G algorithm [8], and 128-



EEA0	128-EEA1	128-EEA2	128-EEA3	EEA4	EEA5	EEA6	EEA7
EIA0	128-EIA1	128-EIA2	128-EIA3	EIA4	EIA5	EIA6	EIA7

Fig. 3 Security and integrity options of 5G NSA

EEA2 and 128-EIA2 mean the 128 bit Advanced Encryption Standard (AES) algorithm [9]. 128-EEA2 uses the AES-Counter (CTR) mode [10], and 128-EIA2 uses the AES-Cipher-based (CMAC) mode [11]. 128-EEA3 and 128-EIA3 mean the ZUC algorithm [12], and EEA/EIA 4 7 are not used. What needs special attention is that during encryption, the plaintext is not encrypted with the key and algorithm, but the key and algorithm are used to generate keystream, and XOR operation is performed for the plaintext and bit level to obtain the ciphertext.

2.2.2 IMS security

IPSec can be applied to the PDN—UE section including IMS. The cryptographic suite of IPSec is defined in RFC 4308—"Cryptographic Suites for IPsec" [13], and Table 1 summarizes the cryptographic algorithms for IPsec, and Table 2 summarizes the cryptographic suite for IPsec.

Table 1 Cryptographic algorithms for IPsec

Cryptographic function	Algorithms
Encryption	HMAC-SHA1/SHA2
	TripleDES-CBC
	AES-CBC
	AES-GCM
	ChaCha20/Poly1305
Authentication	RSA
	ECDSA
	PSK
Key exchange	Diffie-Hellman

Table 2 Cryptographic suite for IPsec

Cryptographic Suite	Algorithms
VPN-A	IPsec encryption—TripleDES-CBC
	IPsec integrity—HMAC-SHA1-96
	Key exchange encryption—TripleDES-CBC
	Key exchange pseudo-random function—HMAC-SHA1
	Key exchange integrity—HMAC-SHA1-96
	Key exchange Diffie-Hellman group—1024-bit modular exp.
VPN-B	IPsec encryption—AES-CBC-128
	IPsec integrity—AES-XCBC-MAC-96
	Key exchange encryption—AES-CBC 128
	Key exchange pseudo-random function—AES-XCBC-PRF-128
	Key exchange integrity—AES-XCBC-MAC-96
	Key exchange Diffie-Hellman group—2048-bit modular exp.

3 Related works

As 5G NSA uses the 4G LTE core network, 4G network vulnerabilities that are not supplemented can be a problem as well. R. P. Jover and V. Marojevic [14] analyzed the vulnerabilities of 4G LTE that can be effective in 5G networks. Among the vulnerabilities of LTE deemed to be able to also affect 5G networks, R. Jover and V. Marojevic [14] describe IMSI exposure, and A. Shaik et al. [15] describe Denial of Service (DoS). S. R. Hussain et al. [16] describe a vulnerability that can perform a downgrade to an insecure connection, and Rupprecht et al. [17] describe a vulnerability that can perform location tracking and DNS hijacking. Fonyi [18] analyzed the security of 5G and attendant vulnerabilities in terms of confidentiality, integrity and availability. Major vulnerabilities are revealed in a vulnerability analysis of a 5G AKA algorithm [19,20] and a study on an MitM attack using a false base station and 5G AKA vulnerability [21]. As for the vulnerability to Vo5G, D. Rupprecht et al. [4] describe call eavesdropping through the keystream reuse vulnerability, and Chlosta et al. [5] describe the vulnerability of eavesdropping and message forgery by inducing null-ciphering. Park et al. [6] describe the vulnerability of disabling media protection by turning off IPsec.

Currently, most of the related research is limited to vulnerability analysis and proposing countermeasures. Most of the reported vulnerabilities have been fixed by hardware and software patches, or by describing supplements to the latest 5G standards. However, this paper found that there are still vulnerabilities in the 5G network as of early 2020 some of which will take a long time to patch or are not easy to respond to right away. Therefore, there is a need for a way to detect and respond to attacks using actual vulnerabilities, not just countermeasure proposals for the security of the current 5G network.

4 Vulnerabilities of 5G-based IoT system

4.1 Reuse of AS keystream

The radio connection between UE and the base station goes into the idle state to save resources if inactivity is detected for a certain period of time. When reactivating the radio connection, UE and the base station generates a new key for encryption. Also, as soon as the call is terminated, the connection used for the call must be removed and a new keystream must be used for each call. As Rupprecht et al. [4] describes, if a call is made immediately after the call is terminated, however the same bearer identity and sequence which reset to 0 may be used to generate a new keystream while generating a new connection, therefore the same keystream may be used. On the other hand, 5G encryption makes cybertext through XOR operation of the keystream and plaintext. Taking advantage of this, if a message knowing the plaintext in the second call is sent when the same keystream is used, it is possible to get the keystream through XOR operation of the plaintext and ciphertext. Accordingly, if the attacker snipped the first user's call and captured the encrypted call, the call details can be decrypted through XOR operation of the keystream obtained from the second call and the user's encrypted call.

4.2 NAS null-ciphering vulnerability

A commercial network allows null-encryption and null-integrity. In this case, all the messages exchanged by the user terminal are transmitted in plaintext, and not only will confidentiality be breached, but also forgery and alteration cannot be verified. So, integrity is not protected either. This option may be applied to emergency calls. In case of an emergency call, even terminals without the Universal Subscriber Identity Module (USIM) must support this function. If the terminal does not have USIM, there is no provisioned encryption key either. So, authentication is performed with null-encryption and null-integrity. On the other hand, except for emergency calls, the standard prescribes that the null-encryption and null-integrity option should not be used in NAS security [22]. However, as Chlosta et al. [5] describes, connection for the null-encryption and null-integrity option is allowed due to errors in the implementation or device settings. In particular, AS security is determined based on the UE Security Capability of the NAS Attach Request message. Accordingly, if connection is made after UE Security Capability is transmitted to the null-encryption and null-integrity option when the NAS Attach Request message is sent, AS connection is also made with null-encryption and null-integrity. As AS security is RAN section, if the attacker has snipping equipment, he/she can easily capture the network traffic of the user terminal through the snipping equipment. Accordingly, a correct response to NAS null-ciphering vulnerability is very important for the normal security of the user terminal.

In general, the user terminal has the null-encryption and null-integrity setting very rarely. Accordingly, the attacker installs a fake base station, and tries to modify the UE Security Capability of the Attach Request message to NULL through the Man in the Middle (MitM) attack. The MitM attack is performed by installing a false base station that can send stronger signals than the mobile carrier's base station to the user terminal. UE usually selects the eNodeB with the highest signal strength and quality or cells on priority frequencies. After all, the user terminal connects to a false base station with stronger signals, not the mobile carrier's base station, and the attacker can perform MitM attack while relaying, forging and altering the message between UE and the mobile carrier's base station. If UE additionally uses a security function like IPsec, despite the null-encryption and null-integrity of MME and the base station, however, encrypted packets can be transmitted, and in this case, the attacker cannot perform eavesdropping and forgery and alteration.

4.3 SIP register message on plaintext and optional use of IPsec

Encryption and integrity verification of the SIP message between UE and IMS may be performed by AS security even if IPsec is not applied. However, M. Chlosta et al.'s attack, described in Sect. 4.2, may be performed, and NAS and AS security may not be applied in some cases. The SIP register message is for registering UE in the IMS server. As this message is sent before the use of IPsec, if AS security is

Table 3 Header fields of register message to attack

Header field name	Modification to
Via	Change IP address
Contact	Change UE URI
To	Change UE URI
From	Change UE URI
Cseq	Change to higher value
Expires	Change to 3600 or 0
Authorization	Change IMSI or UE calling number

not applied, it is always transmitted in plaintext. So, it may be a major target for the attacker's capture, forgery and alteration. The SIP register message includes a variety of information, and Table 3 summarizes the key header fields that the attacker needs to use the message maliciously. Modification of IP, Uniform Resource Identifier (URI), IMSI and UE calling number may lead to abnormal connection, and modification of Cseq and Expires may induce DoS. On the other hand, the section to which IPsec is applied can be largely divided into 2 sections. External communication is performed through SEG, and the SEG-SEG communication section, which is external network connection like different mobile carrier networks connection section, is defined as Za interface. The zb interface includes SEG—Network Entity (NE) and NE—NE communication section. Vo5G communication uses UE—CSCF bearer is one of the NE—SEG communication types [23]. IMS security, which performs Vo5G service, is described in [24]. According to the standard, IPsec must be performed for Za interface unconditionally. On the other hand, only authentication is essential for Zb interface, and encryption through IPsec is optional. Accordingly, for user terminals or internal network connections with IPsec off, connection to which IPsec is not applied by the SEG with no IPsec setting may be established [6].

5 Countermeasures

5.1 Countermeasure for AS vulnerability

There are hundreds of thousands of 5G base stations around the world. Accordingly, installation of security equipment for AS security is burdensome in terms of costs. Accordingly, clear description of security standards and base station patches, not introduction of additional security equipment, are deemed to be desirable. Rupprecht et al. proposed different radio bearer allocation, intra-cell handover and switching between Radio Resource Control (RRC) idle/connected as short-term defense for all calls. However, there are limitations, such as only 32 bearers can be used to prevent the reuse of the keystream due to the 5-bit limit of the bearer field, and the cost of using the additional key derivation function, and latency due to the idle mode. As long-term defense, they proposed the use of an additional layer of security through an additional media encryption function like IPsec. To solve the problem of keystream reuse more fundamentally, we suggest that the standard should describe it in more detail, and abnormal cases of and sequence being reset to 0 with the same bearer identity should be prevented, and it should be supplemented with the base station patch. Also, to be able to respond the potential vulnerabilities of AS security, as Rupprecht et al. proposed, it will be necessary to apply additional media encryption like IPsec.

5.2 Countermeasure for NAS vulnerability

If NSA security is neutralized with null-encryption and null-integrity by the manipulation of UE network capability, AS security can also be neutralized as it depends on UE network capability. The standard prohibits the use of null-encryption and null-integrity [22], but Chlosta et al.'s research and our experiment (Sect. 6.3.1) found vulnerabilities due to the implementation problems of actual equipment of the mobile carrier. Accordingly, it is now necessary to detect NAS security neutralization attempts, and we are proposing a method. Figure 4 is a flow chart of the NAS security neutralization attempt detection technique, and Table 4 summarizes the data used for it. Anomaly detection is largely divided into Attach Request message-based analysis, NSA Security Mode Complete-based analysis and Attach Accept message-based analysis.

Attach Request message-based analysis inspects those cases in which the UE network capability field supports only null-encryption or null-integrity. If only the null option is supported, whether there are previous connection records is checked through the IMSI of the UE, and the previously received UE network capability and the current UE network capability are compared. If the two UE network capabilities are the same, they will be judged to be a security neutralization suspicious channel requiring

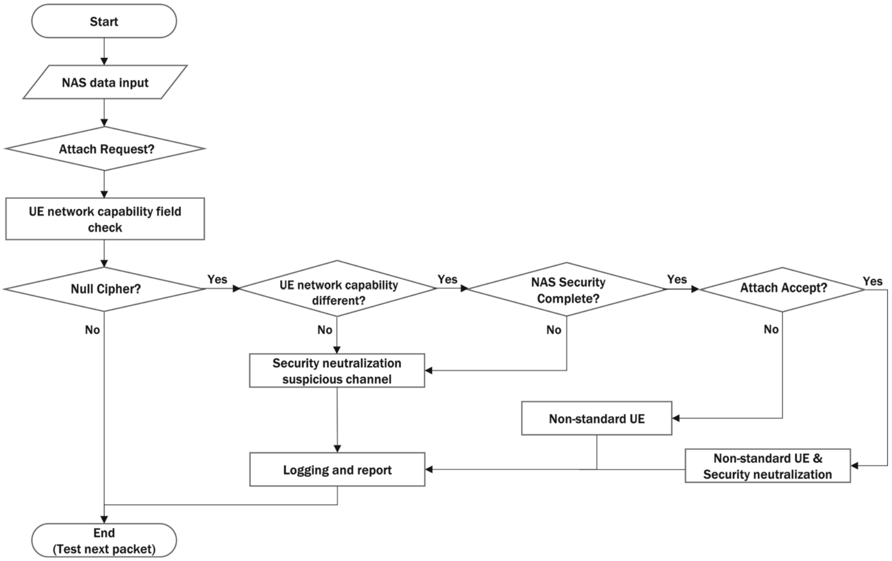


Fig. 4 Flow chart of NAS anomaly detection

Table 4 Required data for NAS anomaly detection

Type	Field	Description
User information	IMSI	Identification of UE
	MSISDN (Mobile Station ISDN)	Phone number of UE
	User IP version	IP version of UE
	User IPv4	IPv4 address of UE
	User IPv6	IPv6 address of UE
	Tracking Area Identity (TAI) List	Base station list which UE can access for analyzing the UE location
NSA message information	Attach Request Time	Time of Attach Request message
	Attach Reject Cause	Cause of Attach Reject message
	Attach Request Type	Type of Attach Request
		1: EPS attach
		2: combined EPS/IMSI attach
		6: EPS emergency attach
	Security Mode Command Time	Time of Security Mode Command message
	Security Mode Reject Cause	Cause of Security Mode Reject message
	UE network capability	EEA, EIA configuration of UE
	Selected EEA/EIA	Selected EEA/EIA mode by MME

continuous management, and logging will be performed. The logging includes the user information in Table 4, which was used for anomaly detection, and the detection type and detection time. Besides, if the two UE network capabilities are different, the following steps will be performed for more accurate judgment.

NSA Security Mode Complete-based analysis analyzes the response message to the NSA Security Mode Command message from UE. If the NSA Security Mode Reject message is received from UE, UE checked the replayed UE network capability and confirmed that it is different from the UE network capability it transmitted. In this case, as in the previous stage, it will be judged to be a security neutralization suspicious channel requiring continuous management, and logging will be performed. Besides, if the NSA Security Mode Complete message is received, the following steps will be performed for more accurate judgment.

Attach Accept-based analysis checks if MME transmitted the Attach Accept message and a security neutralization channel is generated between UE and MME. If Attach Reject occurred, the UE which was not implemented according to the standard will be judged to be non-standard UE, and logging will be performed. If the Attach Accept message was transmitted, and UE—MME connection was established, it will be judged to be a non-standard UE and security neutralization channel, and logging will be performed. As a follow-up measure for detection, UE information on the non-standard UE and security neutralization channel will be transmitted to the core network like HSS, and it may be disconnected. Additionally, it is judged that a malicious use, not a general user, transmitted the traffic of the security neutralization channel by faking the UE, and the charging records on the traffic of the UE can be excluded.

Detection equipment can detect anomalies of the NSA security setup by deploying additional equipment between UE and MME or adding the security function to MME.

5.3 Countermeasure for IMS-IPSec vulnerability

As there are terminals that do not use IPsec by default like iPhone, in the current mobile environment, there are many devices that do not use IPsec. Also, as devices which used to use IPsec may switch to iPhone, regardless of whether IPsec is used, it cannot be said to be an abnormal connection. If the IPsec function is turned off, a device that can use IPsec as the attacker changes the settings or the user sets it up negligently, however, it can use IPsec by transmitting the support function of the device itself, not the terminal settings. As an element necessary for 5G security is stronger than IPsec, to resolve the issue about the use of IPsec, the standard must change the security environment of the terminal by changing optional use to mandatory use in the long run. On the other hand, as forgery and alteration of the SIP register messages that are likely to occur is a security issue that must be responded immediately, we must detect anomalies by tracking the key information of UE as in Table 3. Detection equipment can detect anomalies of IMS by deploying additional equipment between UE and IMS or adding the security function to IMS CSCF.

5.4 Countermeasure for false base station—TR 33.809

Many attacks including [5,21] use a false base station between UE and the base station to establish a malicious connection. By doing so, the attacker can trigger DoS for the communication between UE and the network, transmit rogue services and expose subscriber privacy. As false base station-based attacks are continuously reported, to respond to it, starting with November 19, 2018, TR 33.809—Study on 5G security enhancements against false base stations version 0.1.0, 3GPP recently performed the August 31, 2020 version 0.10.0 [25] work. Still TR 33.809 is an uncompleted standard, but version 0.10.0 is describing 7 key security issues and 23 candidate solutions to respond to it. They are summarized in Table 5. If the details of TR 33.809 are applied, many attacks including [5,21] can be blocked fundamentally.

6 Countermeasure implementation and results

Section 6 describes the test environment, scope, the eavesdropping scenarios, the result of eavesdropping experiment, and the result of eavesdropping detection.

Table 5 Key issues and candidate solutions of TR 33.809 against false base station

Key issue	Security threats	Candidate solution
#1 Security of unprotected unicast message	DoS attack on UE Limited network service	#1 Protection for the UE capability transfer
		#2 Protection of RRCReject message in RRC_INACTIVE state
		#3 Protection of uplink UECapabilityInformation RRC message
		#9 Using symmetric algorithm with assistance of USIM and home network
		#10 Protection on the unicast message based on ECDH
		#11 Certificate based solution against false base station
		#12 ID based solution against false base station
		#13 Protecting RRCResumeRequest against MitM
		#16 Protection of RRC reject message
		#17 Integrity protection of the whole RRCResumeRequest message
		#21 Certificate based solution against false base station for non-public networks

Table 5 continued

Key issue	Security threats	Candidate solution
#2 Security protection of system information	DoS attack on UE Rogue services	#7 Verification of authenticity of the cell
		#11 Certificate based solution against false base station
		#12 ID based solution against false base station
		#14 Shared key based MIB/SIBs protection
		#19 AS security based MIB/SIBs integrity information provided by gNB
		#20 Digital signing network function
#3 Network detection of false base stations	DoS attack on network DoS attack on UE Fraud Subscriber privacy	#4 Enriched measurement reports
		#6 Avoiding UE connecting to false base station during HO
		#8 Network detection of nearby false bast stations from call statistics and measurements
		#18 Avoiding UE connecting to false base station during conditional handover
		#22 Detecting fake base stations based on UE positioning measurements
#4 Protection against SON poisoning attempts	DoS attack on network DoS attack on UE	TBD
#5 Mitigation the authentication relay attack	Deception Location history poisoning	#5 Mitigation against the authentication relay attack
	DoS attack on UE Attack on SON	#15 Mitigation against the authentication relay attack with different PLMNs
#6 Resistance to radio jamming	DoS attack on UE DoS attack on network	TBD
#7 Protection against Man-	DoS attack on UE in-the-Middle false gNB attacks	#23 Cryptographic CRC to avoid MitM relay nodes

Table 6 Testing components for eavesdropping

Testing components	Component details
Test UE device	Galaxy S10 (SM-G977N)
UE Android OS version	9(Pie)
UE kernel version	4.14.85
Malicious UE	srsUE [26]
False base station	USRP B210 [27]
Packet dump	tcpdump
NAS Packet	analysis Wireshark
NAS packet generator	Software Defined Radio (SDR)
SIP packet modification	sendip
AS packet dump and analysis	OPTis-S [28]
Testing target	Network of mobile carrier A, B and C

Table 7 IDS performance

IDS components	Component details
OS	CentOS Linux 7.6.1810
CPU	Intel Xenon CPU E5645 2.4 GHz
RAM	132 GB
Traffic collecting rate	33.07 Gbps
Session processing rate	107390 session/s

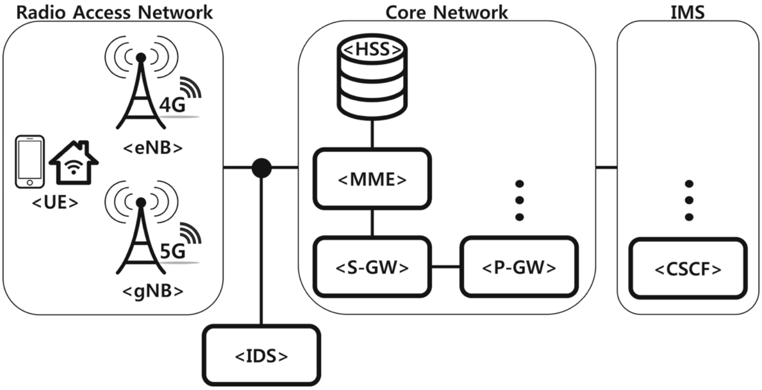


Fig. 5 5G NSA network and IDS

6.1 Test environment and scope

Table 6 summarizes the equipment used for the eavesdropping experiment, and Table 7 summarizes the performance of the IDS equipment for detection of eavesdropping.

The experiment on AS communication confirmed that eavesdropping due to keystream reuse is valid for mobile carrier A and B. As explained in Sect. 5.1, however, it is unreasonable in terms of cost to install anomaly detection equipment for the communication between UE and the base station. Accordingly, the scope of IDS excludes AS security of the RAN section, and IDS aimed to perform UE communication, capture and anomaly detection inside the 5G NSA core network as illustrated in Fig. 5.

6.2 Eavesdropping scenario on 5G-based IoT system

Section 6.2 describes the eavesdropping scenario using the vulnerabilities described in Sect. 4.

6.2.1 Eavesdropping scenarios on 5G NAS network

Figure 6 is the sequence diagram of the eavesdropping scenario using NAS null-ciphering vulnerabilities. The attacker's precondition is that the MitM attack performance environment should be created and the victim UE does not use any additional media protection like IPsec. For successful MitM attacks, a tool for installing a false base station that can send stronger signals than eNB and gNB to the victim UE and manipulate the network packets of the victim UE and MME. If the MitM attack environment is successfully configured, the victim UE will send the Attach Request message to the false base station. The attacker will transmit only EEA0 (null-encryption) and EIA0 (null-integrity) by setting the UE network capability of the Attach Request. For authentication, the attacker will relay following messages. If null-ciphering communication is established in the UE—MME NAS connection

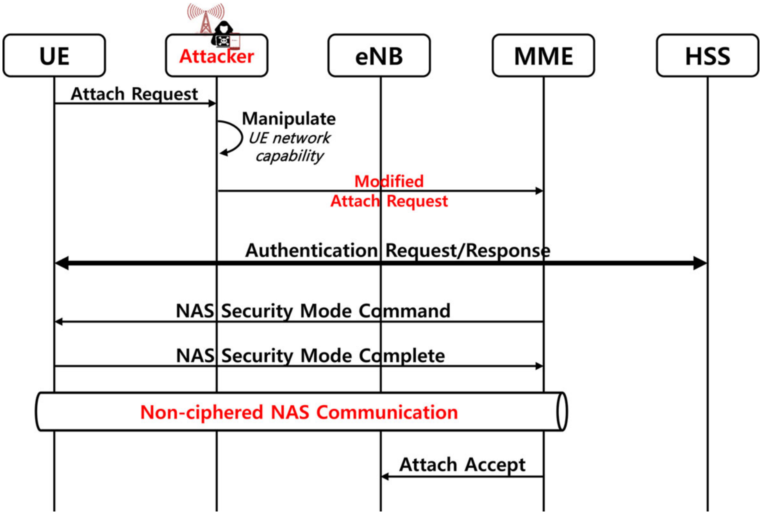

UE
Attacker
eNB
MME
HSS
Attach Request
Manipulate
UE network
capability
Modified
Attach Request
Authentication Request/Response
NAS Security Mode Command
NAS Security Mode Complete
Non-ciphered NAS Communication
Attach Accept

Fig. 6 Sequence diagram of eavesdropping using NAS null-ciphering vulnerability

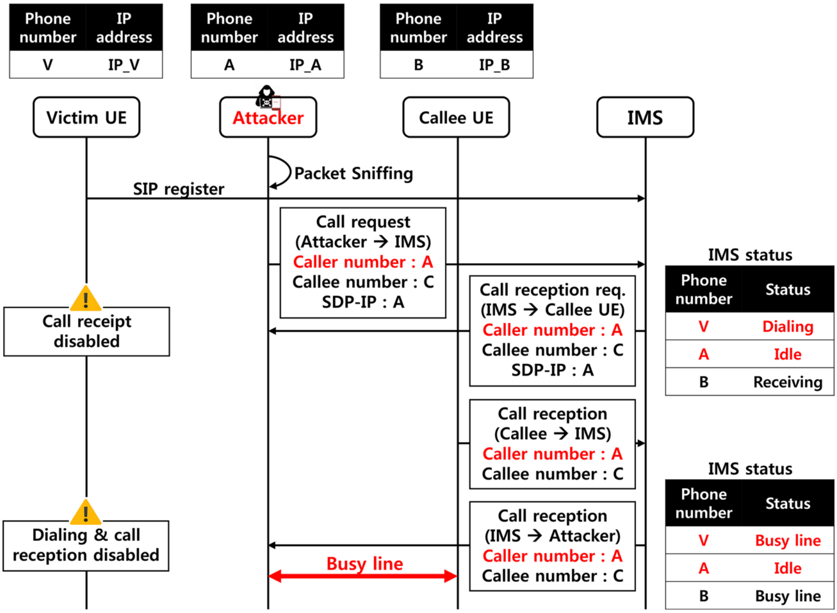


Fig. 7 Sequence diagram of phone call charging avoidance using IPsec off vulnerability

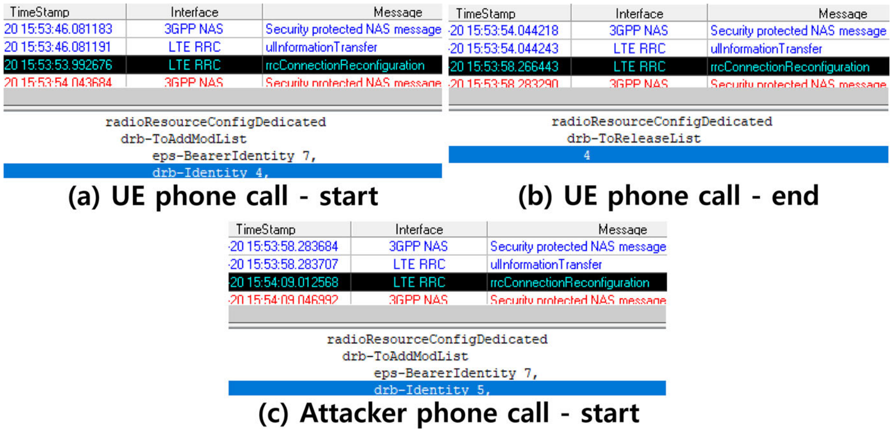
section, null-ciphering communication will also be established in the eNB and AS connection section, and then the communication settings of eNB will be sent to gNB, and gNB communication will also be established as null-ciphering communication. Accordingly, the attacker can freely manipulate the messages of the victim UE through continuous MitM attacks, and conduct a wide range of malicious actions from DoS to abnormal use.

6.2.2 Eavesdropping scenarios on 5G IMS network

As for IPsec off vulnerabilities, the phone call charge avoidance scenario will be described by manipulating the eavesdropping and SIP message. Figure 7 is the sequence diagram of the phone call charge avoidance scenario using IPsec off vulnerabilities. The precondition of the attacker is the configuration of the vulnerable UE environment with the IPsec option off and the UE network traffic snipping environment. If snipping is done in the RAN section, plaintext must be acquired through tcpdump from the UE or AS security neutralization must be performed using NAS null-ciphering vulnerabilities. If the victim UE with the IPsec option off sends the SIP register message to IMS, the attacker will snip this message and saves various information on the victim UE. If the victim UE finishes registration, it will not use IPsec, and if the attacker can neutralize AS security, the attacker can disguise as the victim UE and send a message to IMS. Accordingly, if the attacker changes the originating number of his/her SIP invite message into the number of the victim UE and transmits it as illustrated in Fig. 7, a phone call will be established with the information of the victim UE, but the attacker will make the phone call. As a result, the victim UE cannot

Table 8 Eavesdropping attack results

Eavesdropping type	Mobile carrier A	Mobile carrier B	Mobile carrier C
AS	O	O	X
NAS	O	O	O
IMS	X	O	O



```
TimeStamp           Interface   Message
20 15:53:46.081183  3GPP NAS    Security protected NAS message
20 15:53:46.081191  LTE RRC     ulInformationTransfer
20 15:53:53.992676  LTE RRC     rrcConnectionReconfiguration
20 15:53:54.043684  3GPP NAS    Security protected NAS message

radioResourceConfigDedicated
  drb-ToAddModList
      eps-BearerIdentity 7,
      drb-Identity 4,
```

(a) UE phone call - start

```
TimeStamp           Interface   Message
20 15:53:54.044218  3GPP NAS    Security protected NAS message
20 15:53:54.044243  LTE RRC     ulInformationTransfer
20 15:53:58.266443  LTE RRC     rrcConnectionReconfiguration
20 15:53:58.283290  3GPP NAS    Security protected NAS message

radioResourceConfigDedicated
  drb-ToReleaseList
    4
```

(b) UE phone call - end

```
TimeStamp           Interface   Message
20 15:53:58.283684  3GPP NAS    Security protected NAS message
20 15:53:58.283707  LTE RRC     ulInformationTransfer
20 15:54:09.012568  LTE RRC     rrcConnectionReconfiguration
20 15:54:09.046992  3GPP NAS    Security protected NAS message

radioResourceConfigDedicated
  drb-ToAddModList
      eps-BearerIdentity 7,
      drb-Identity 5,
```

(c) Attacker phone call - start

Fig. 8 Results of AS keystream reuse attack—mobile carrier C's network

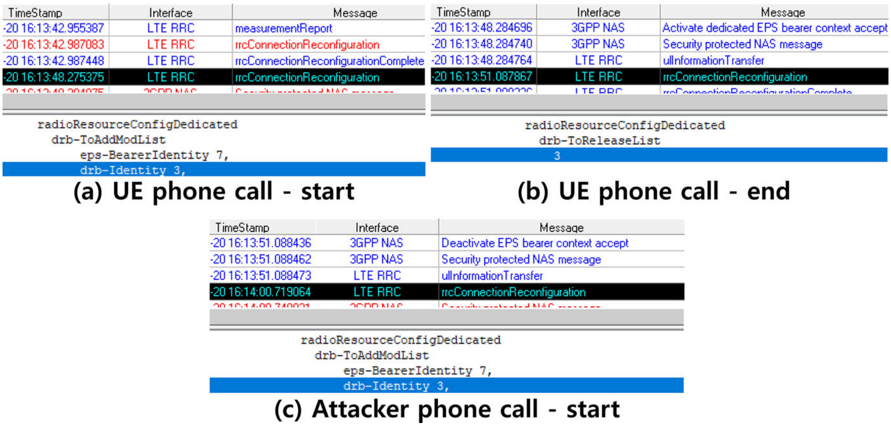
make a phone call while the attacker is talking on the phone, and the charge for the attacker's phone call will be charged to the victim UE.

6.3 Implementation results

6.3.1 Eavesdropping attack results

Table 8 shows the results of the eavesdropping tests. A "O" indicates a vulnerable to eavesdropping. Mobile carrier A's network is vulnerable to AS keystream reuse attack and NAS null-ciphering attack. Mobile carrier B's network is vulnerable to all 3 attacks and Mobile carrier C's network is vulnerable to NAS null-ciphering attack and IPsec disabling attack.

Figure 8 shows the results of an AS keystream reuse attack on mobile carrier C's network. The AS packets were captured and analyzed using OPTis-S[28] tools. Figure 8a shows the effects upon the victim UE's phone call. The connection was established using Data Radio Bearer (DRB) identity 4. After the phone call was completed, the DRB 4 is released (Fig. 8b) and an incremented DRB identity 5 is created for the attacker's phone call. Therefore, both keystreams are different due to there being different DRB identities which render keystream generation material and keystream reuse attack impossible. However, Fig. 9 shows the results of an AS keystream reuse attack on mobile carrier A and B's network where keystream reuse is possible because mobile



TimeStamp	Interface	Message
-20 16:13:42.955387	LTE RRC	measurementReport
-20 16:13:42.987083	LTE RRC	rrcConnectionReconfiguration
-20 16:13:42.987448	LTE RRC	rrcConnectionReconfigurationComplete
-20 16:13:48.275375	LTE RRC	rrcConnectionReconfiguration

```
radioResourceConfigDedicated
  drb-ToAddModList
      eps-BearerIdentity 7,
      drb-Identity 3,
```

(a) UE phone call - start

TimeStamp	Interface	Message
-20 16:13:48.284696	3GPP NAS	Activate dedicated EPS bearer context accept
-20 16:13:48.284740	3GPP NAS	Security protected NAS message
-20 16:13:48.284764	LTE RRC	ulInformationTransfer
-20 16:13:51.087867	LTE RRC	rrcConnectionReconfiguration

```
radioResourceConfigDedicated
  drb-ToReleaseList
    3
```

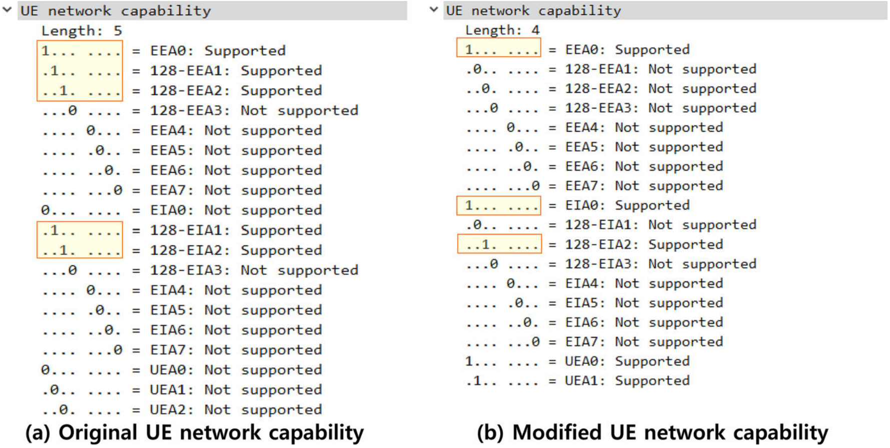
(b) UE phone call - end

TimeStamp	Interface	Message
-20 16:13:51.088436	3GPP NAS	Deactivate EPS bearer context accept
-20 16:13:51.088462	3GPP NAS	Security protected NAS message
-20 16:13:51.088473	LTE RRC	ulInformationTransfer
-20 16:14:00.719064	LTE RRC	rrcConnectionReconfiguration

```
radioResourceConfigDedicated
  drb-ToAddModList
      eps-BearerIdentity 7,
      drb-Identity 3,
```

(c) Attacker phone call - start

Fig. 9 Results of AS keystream reuse attack—mobile carrier A and B’s network



```
v UE network capability
    Length: 5
    1... .... = EEA0: Supported
    .1.. .... = 128-EEA1: Supported
    ..1. .... = 128-EEA2: Supported
    ...0 .... = 128-EEA3: Not supported
    .... 0... = EEA4: Not supported
    .... .0.. = EEA5: Not supported
    .... ..0. = EEA6: Not supported
    .... ...0 = EEA7: Not supported
    0... .... = EIA0: Not supported
    .1.. .... = 128-EIA1: Supported
    ..1. .... = 128-EIA2: Supported
    ...0 .... = 128-EIA3: Not supported
    .... 0... = EIA4: Not supported
    .... .0.. = EIA5: Not supported
    .... ..0. = EIA6: Not supported
    .... ...0 = EIA7: Not supported
    0... .... = UEA0: Not supported
    .0.. .... = UEA1: Not supported
    ..0. .... = UEA2: Not supported
```

(a) Original UE network capability

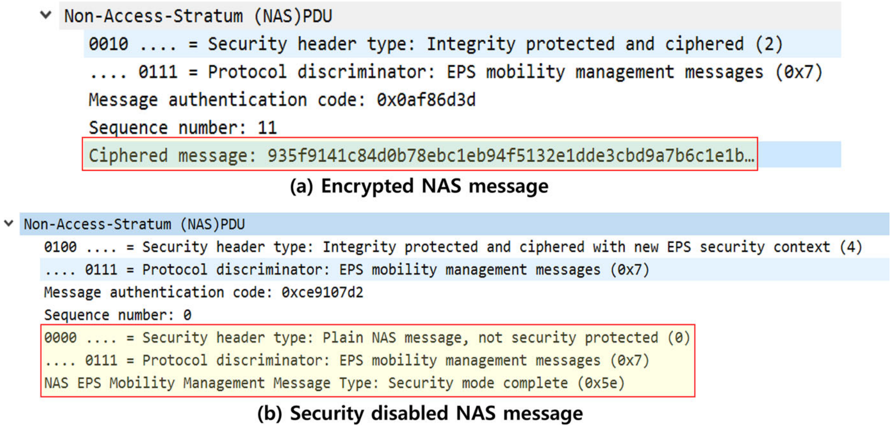
```
v UE network capability
    Length: 4
    1... .... = EEA0: Supported
    .0.. .... = 128-EEA1: Not supported
    ..0. .... = 128-EEA2: Not supported
    ...0 .... = 128-EEA3: Not supported
    .... 0... = EEA4: Not supported
    .... .0.. = EEA5: Not supported
    .... ..0. = EEA6: Not supported
    .... ...0 = EEA7: Not supported
    1... .... = EIA0: Supported
    .0.. .... = 128-EIA1: Not supported
    ..1. .... = 128-EIA2: Supported
    ...0 .... = 128-EIA3: Not supported
    .... 0... = EIA4: Not supported
    .... .0.. = EIA5: Not supported
    .... ..0. = EIA6: Not supported
    .... ...0 = EIA7: Not supported
    1... .... = UEA0: Supported
    .1.. .... = UEA1: Supported
```

(b) Modified UE network capability

Fig. 10 NAS UE network capability modification results

carrier A and B’s network only uses DRB identity 3. In the case of AS keystream reuse, we only tested keystream reuse vulnerability on the mobile carriers’ network because the RAN network boundary is not within the scope of our IDS.

Figure 10 illustrates the captured packets which are confirmed by wireshark after manipulating UE network capability for NAS security neutralization. Figure 10b shows that the values of both EEA and EIA are changed as compared to Fig. 10a, and the EEA of Fig. 10b’s UE network capability only supports null-encryption. Figure 11 illustrates the captured packets which are transmitted between UE and MME after manipulating UE network capability. Figure 11a illustrates messages ciphered by using normal security, whereas Fig. 11b messages transmitted in plaintext as security was disabled. NAS null-ciphering attacks were performed for 1,989 sessions out of a total of 120,000 sessions generated with SDR.



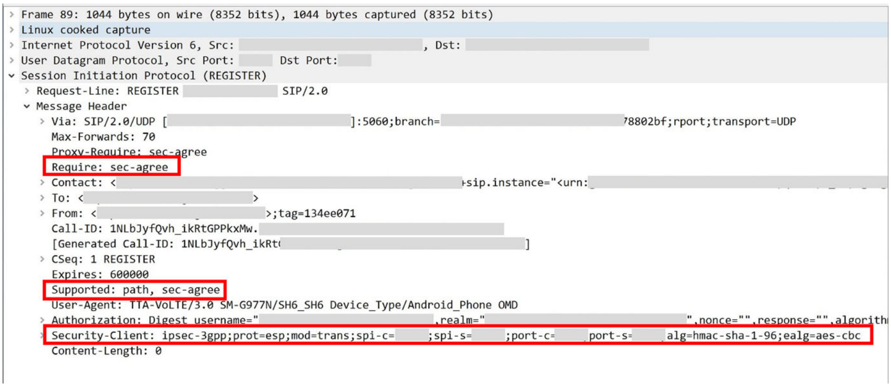
```
⌄ Non-Access-Stratum (NAS)PDU
    0010 .... = Security header type: Integrity protected and ciphered (2)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
    Message authentication code: 0x0af86d3d
    Sequence number: 11
    Ciphered message: 935f9141c84d0b78ebc1eb94f5132e1dde3cbd9a7b6c1e1b…
```

(a) Encrypted NAS message

```
⌄ Non-Access-Stratum (NAS)PDU
    0100 .... = Security header type: Integrity protected and ciphered with new EPS security context (4)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
    Message authentication code: 0xce9107d2
    Sequence number: 0
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
    NAS EPS Mobility Management Message Type: Security mode complete (0x5e)
```

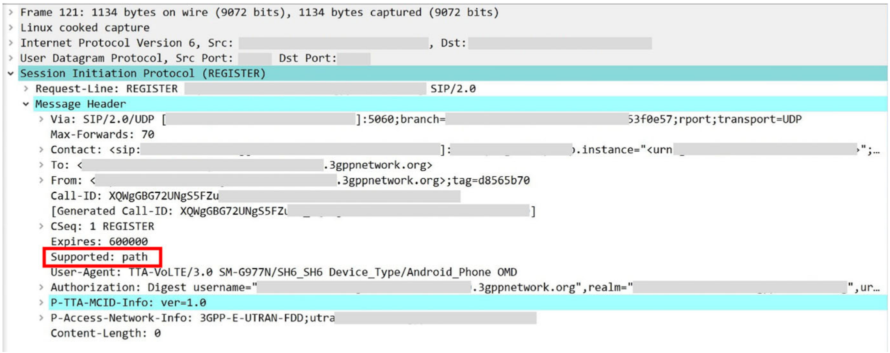
(b) Security disabled NAS message

Fig. 11 NAS security neutralization results—NAS message



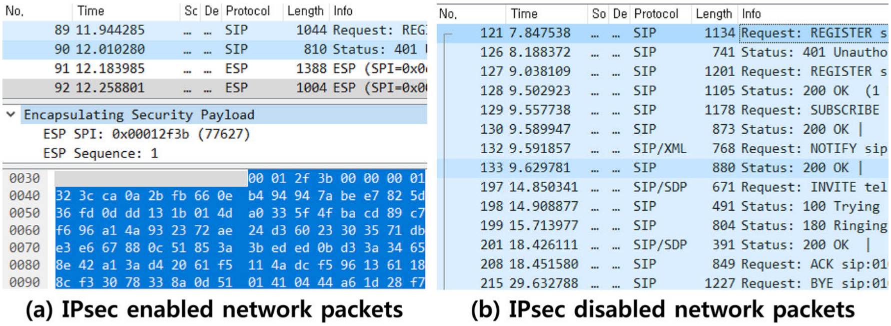
```
> Frame 89: 1044 bytes on wire (8352 bits), 1044 bytes captured (8352 bits)
> Linux cooked capture
> Internet Protocol Version 6, Src: [redacted], Dst: [redacted]
> User Datagram Protocol, Src Port: [redacted] Dst Port:[redacted]
⌄ Session Initiation Protocol (REGISTER)
  > Request-Line: REGISTER [redacted] SIP/2.0
  ⌄ Message Header
    > Via: SIP/2.0/UDP [[redacted]]:5060;branch=[redacted]78802bf;rport;transport=UDP
      Max-Forwards: 70
      Proxy-Require: sec-agree
      Require: sec-agree
    > Contact: <[redacted]+sip.instance="<urn:[redacted]
    > To: <[redacted]>
    > From: <[redacted]>;tag=134ee071
      Call-ID: 1NLbJyfQvh_ikRtGPPkxMw.[redacted]
      [Generated Call-ID: 1NLbJyfQvh_ikRt[redacted]]
    > CSeq: 1 REGISTER
      Expires: 600000
      Supported: path, sec-agree
      User-Agent: TTA-VoLTE/3.0 SM-G977N/SH6_SH6 Device_Type/Android_Phone OMD
    > Authorization: Digest username="[redacted],realm="[redacted]",nonce="",response="",algorith
    > Security-Client: ipsec-3gpp;prot=esp;mod=trans;spi-c=[redacted];spi-s=[redacted];port-c=[redacted] port-s=[redacted] alg=hmac-sha-1-96;ealg=aes-cbc
      Content-Length: 0
```

Fig. 12 SIP register message of IPsec enabled UE



```
> Frame 121: 1134 bytes on wire (9072 bits), 1134 bytes captured (9072 bits)
> Linux cooked capture
> Internet Protocol Version 6, Src: [redacted], Dst: [redacted]
> User Datagram Protocol, Src Port: [redacted] Dst Port:[redacted]
⌄ Session Initiation Protocol (REGISTER)
  > Request-Line: REGISTER [redacted] SIP/2.0
  ⌄ Message Header
    > Via: SIP/2.0/UDP [[redacted]]:5060;branch=[redacted]53f0e57;rport;transport=UDP
      Max-Forwards: 70
    > Contact: <sip:[redacted]]:[redacted]).instance="<urn[redacted]>";…
    > To: <[redacted].3gppnetwork.org>
    > From: <[redacted].3gppnetwork.org>;tag=d8565b70
      Call-ID: XQWgGBG72UNgS5FZu[redacted]
      [Generated Call-ID: XQWgGBG72UNgS5FZ[redacted]]
    > CSeq: 1 REGISTER
      Expires: 600000
      Supported: path
      User-Agent: TTA-VoLTE/3.0 SM-G977N/SH6_SH6 Device_Type/Android_Phone OMD
    > Authorization: Digest username="[redacted].3gppnetwork.org",realm="[redacted]",ur…
    > P-TTA-MCID-Info: ver=1.0
    > P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utra[redacted]
      Content-Length: 0
```

Fig. 13 SIP register message of IPsec disabled UE



```
No.  Time        Sc De Protocol Length Info
 89 11.944285   ... ... SIP     1044 Request: REG
 90 12.010280   ... ... SIP      810 Status: 401 
 91 12.183985   ... ... ESP     1388 ESP (SPI=0x0
 92 12.258801   ... ... ESP     1004 ESP (SPI=0x0

˅ Encapsulating Security Payload
    ESP SPI: 0x00012f3b (77627)
    ESP Sequence: 1

0030                           00 01 2f 3b 00 00 00 01
0040  32 3c ca 0a 2b fb 66 0e  b4 94 94 7a be e7 82 5d
0050  36 fd 0d dd 13 1b 01 4d  a0 33 5f 4f ba cd 89 c7
0060  f6 96 a1 4a 93 23 72 ae  24 d3 60 23 30 35 71 db
0070  e3 e6 67 88 0c 51 85 3a  3b ed ed 0b d3 3a 34 65
0080  8e 42 a1 3a d4 20 61 f5  11 4a dc f5 96 13 61 18
0090  8c f3 30 78 33 8a 0d 51  01 41 04 44 a6 1d 28 f7
```

(a) IPsec enabled network packets

```
No.  Time        So De Protocol Length Info
121 7.847538    ... ... SIP     1134 Request: REGISTER s
126 8.188372    ... ... SIP      741 Status: 401 Unautho
127 9.038109    ... ... SIP     1201 Request: REGISTER s
128 9.502923    ... ... SIP     1105 Status: 200 OK  (1
129 9.557738    ... ... SIP     1178 Request: SUBSCRIBE
130 9.589947    ... ... SIP      873 Status: 200 OK |
132 9.591857    ... ... SIP/XML  768 Request: NOTIFY sip
133 9.629781    ... ... SIP      880 Status: 200 OK |
197 14.850341   ... ... SIP/SDP  671 Request: INVITE tel
198 14.908877   ... ... SIP      491 Status: 100 Trying
199 15.713977   ... ... SIP      804 Status: 180 Ringing
201 18.426111   ... ... SIP/SDP  391 Status: 200 OK  |
208 18.451580   ... ... SIP      849 Request: ACK sip:01
215 29.632788   ... ... SIP     1227 Request: BYE sip:01
```

(b) IPsec disabled network packets

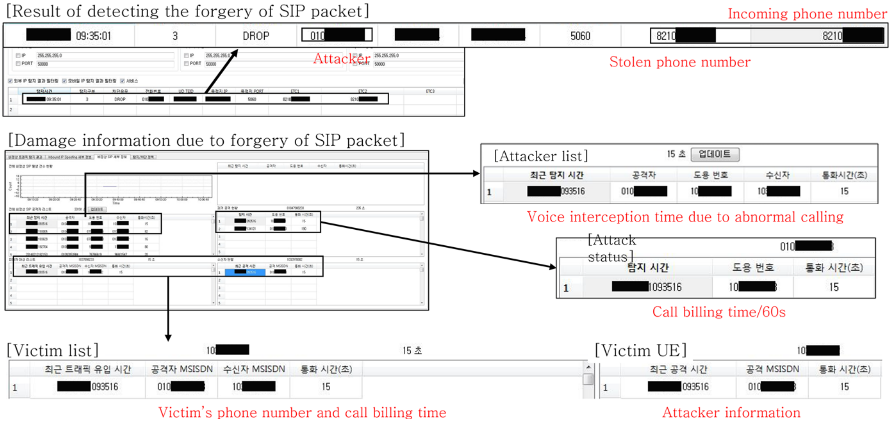
Fig. 14 IMS security neutralization results—SIP messages

Figure 12 illustrates the SIP register message that normally performs IPsec. Like the red box in Fig. 10, the request for setting IPsec is performed. On the other hand, Fig. 13 illustrates the SIP register message sent by UE with disabled IPsec. Unlike Fig. 12 the fields and values related security are missing. As a result, the connection in Fig. 12 guarantees confidentiality by transmitting the payload encapsulated by IPsec as in Fig. 14a, whereas the connection in Fig. 13 cannot guarantee confidentiality as it is transmitted in plain text as in Fig. 14b. However, mobile carrier C's core network does not use IPsec whether UE uses IPsec or not. SIP message modification attacks were performed for 621 sessions.

The security issues identified through the test were delivered to mobile carrier A, B and C, and security issues were patched or are being patched.

6.3.2 IDS detection results

The IDS we developed is located in front of the core network, and detected anomalies by receiving the communication among UE, MME and S-GW through mirroring. As



[Result of detecting the forgery of SIP packet]

[redacted] 09:35:01	3	DROP	010[redacted]	[redacted]	[redacted]	5060	8210[redacted] 8210[redacted]

[Damage information due to forgery of SIP packet]

[Attacker list] 15 초 업데이트

	최근 탐지 시간	공격자	도용 번호	수신자	통화시간(초)
1	[redacted]093516	010[redacted]	10[redacted]	10[redacted]	15

[Attack status] 010[redacted]

	탐지 시간	도용 번호	통화 시간(초)
1	[redacted]1093516	10[redacted]	15

[Victim list] 10[redacted] 15 초

	최근 트래픽 유입 시간	공격자 MSISDN	수신자 MSISDN	통화 시간(초)
1	[redacted]093516	010[redacted]	10[redacted]	15

[Victim UE] 10[redacted]

	최근 공격 시간	공격 MSISDN	통화 시간(초)
1	[redacted]093516	010[redacted]	15

Fig. 15 IDS detection result example—SIP message modification

a result, all 1989 NAS null-ciphering attacks performed for 120,000 sessions and 621 SIP message modification attacks were detected. Figure 15 illustrates the log screen generated when IDS detected modification of the SIP message. The log information stores not only the result of SIP message detection, but also the information on the attacked UE and negative charging information for adjusting the charging information of victim UE.

7 Conclusion

Security analysis for 5G NSA networks was performed in response to security risks such as eavesdropping. The 5G NSA network was largely divided into the AS, NAS, and IMS connection sections where the vulnerabilities and countermeasures for each section were analyzed and proposed. Keystream reuse, null-encryption & null-integrity vulnerabilities are consequential threats that breach confidentiality. To verify and validate a countermeasure, it is necessary to perform attacks and security breaches on an actual mobile carrier network. A countermeasure that was developed in this paper successfully functioned as IDS and detected controlled attacks.

It is currently estimated that approximately 20 billion IoT devices are connected to the internet. With the introduction of SA networks, IoT devices that can be widespread using mMTC and URLLC will be shortly introduced to the public. There is an emphasis on cybersecurity, as technological advances though enhances industries, breeds new opportunities for security breaches. Security designs must be done in consideration of various security functions, including the countermeasures against the security issues described in this paper.

Acknowledgements This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2019-0-00793, Intelligent 5G Core Network Abnormal Attack Detection & Countermeasure Technology Development.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. IoT Industrial Devices, Edge of 2020 in Industrial IoT—forecast, 2020.06.01. https://iot-industrial-devices.com/edge-of-2020-in-industrial-iot-forecast/. Accessed 15 Sep 2020

2. No W (2019) Ministry of science and ICT central radio management service, number of 5G base station in, 2019.09.05
3. Wong S (2020) Number of 5G base stations in Chana 2019–2024, statista, 2020.05.27
4. Rupprecht D et al. Call me maybe: eavesdropping encrypted LTE calls with ReVoLTE. In: 29th USENIX security symposium (USENIX security 20)
5. Chlosta M et al (2019) LTE security disabled: misconfiguration in commercial networks. In: Proceedings of the 12th conference on security and privacy in wireless and mobile networks
6. Park S et al (2020) Security problems of 5G voice communication. In: The 21st world conference on information security applications (WISA)
7. Rosenberg J et al (2002) SIP: session initiation protocol. RFC 3261
8. Third Generation Partnership Project, Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications, TS 35.215, 2020.07.10
9. National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, 2001.11.26
10. Dworkin M (2001) Recommendation for Block Cipher Modes of Operation, National Institute of Standards and Technology, NIST Special Publication 800-38A
11. Dworkin M (2005) Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology, NIST Special Publication 800-38B
12. Third Generation Partnership Project, Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications, TS 35.221, 2020.07.10
13. Manral V (2007) Cryptographic algorithm implementation requirements for encapsulating security payload (ESP) and authentication header (AH), Network Working Group, RFC 4835
14. Jover RP, Marojevic V (2019) Security and protocol exploit analysis of the 5G specifications. IEEE Access 7:24956–24963
15. Shaik A, Borgaonkar R, Asokan R, Niemi V, Seifert J-P (2016) Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In: Proceedings of the 23rd annual network and distributed system security symposium (NDSS)
16. Hussain SR, Chowdhury O, Mehnaz S, Bertino E (2018) LTEInspector: a systematic approach for adversarial testing of 4G LTE. In: Proceedings of the symposium network and distributed system security (NDSS), pp 18–21
17. Rupprecht D, Kohls K, Holz T, Pöpper C (2019) Beaking LTE on layer two. In: Proceedings of the IEEE symposium security, privacy (SP)
18. Fonyi S (2020) Overview of 5G security and vulnerabilities. Cyber Defense Rev 5(1):117–134
19. Cremers C, Dehnel-Wild M (2019) Component-based formal analysis of 5G-AKA: channel assumptions and session confusion. In: Network and distributed systems security (NDSS) symposium 2019. https://doi.org/10.14722/ndss.2019.23394
20. Borgaonkar R, Hirschi L, Park S (2019) Shaik A (2019) New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. Proc Priv Enhanc Technol 3:108–27. https://doi.org/10.2478/popets-2019-0039
21. Basin D et al (2018) A formal analysis of 5G authentication. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security. ACM, pp 1383–1396
22. Third Generation Partnership Project, System Architecture Evolution (SAE); Security architecture, TS 33.401, 2020.07.10
23. Third Generation Partnership Project, Network Domain Security (NDS); IP network layer security, TS 33.210, 2020.07.10
24. Third Generation Partnership Project, IP Multimedia Subsystem (IMS) media plane security, TS 33.328, 2020.07.10
25. Third Generation Partnership Project, Study on 5G security enhancements against false base stations version, TR 33.809, 2020.08.31
26. srsLTE. https://github.com/srsLTE/srsLTE. Accessed 15 Sep 2020
27. USRP B210. https://www.ettus.com/product/details/UB210-KIT. Accessed 15 Sep 2020
28. OPTis-S. https://www.dtaq.re.kr/_custom/dtaq/_common/board/download.jsp?attach_no=192170 Accessed 15 Sep 2020