IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 June 2022, accepted 19 June 2022, date of publication 29 June 2022, date of current version 18 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3187053

Session Management for Security Systems in 5G Standalone Network

SEONGMIN PARK[1,2], **SUNGMOON KWON**[1], **YOUNGKWON PARK**[1], **DOWON KIM**[1], **AND ILSUN YOU**[2], **(Senior Member, IEEE)**

[1]Korea Internet & Security Agency, Naju-si 58324, South Korea
[2]Department of Financial Information Security, Kookmin University, Seoul 80523, South Korea

Corresponding author: Ilsun You (isyou@kookmin.ac.kr)

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

ABSTRACT As 5G telecom services evolve rapidly across a broad technological environment, network security in 5G landscape emerges as a critically challenging issue. One of typical network security tools is an intrusion prevention system (IPS) that monitors a network for malicious activity across the cyber-attack chain and takes action to prevent it. Vulnerabilities in 5G core networks become more varied and protocols become increasingly complex, whereby conventional Next Generation Firewall (NGFW) is not enough anymore to respond to cyber attacks. As a typical 5G vulnerability attack, PFCP-in-GTP and IPSec disable attack are highly complex to detect and cannot identify attackers without integrated session management. However, the 5G core network uses various protocols such as Non-Access Stratum (NAS), Hyper Text Transfer Protocol (HTTP), Packet Forwarding Control Protocol (PFCP), and GPRS Tunnelling Protocol (GTP), and packets of the interface used by each protocol are managed as identities that are difficult to identify. Analyzing the relationship of these interfaces in real time is an important key to integrated session management. In addition, unlike existing 4G, as 3rd Generation Partnership Project (3GPP) specs mandate encrypting 5G Standalone (SA) user IDs, it is much more difficult to identify from which user traffic has occurred in IPSs exclusive for cellular network. With regard to the above subject, this paper introduces an efficient session management scheme for users not affordable in conventional NFGW but necessarily useful for security systems in 5G SA. Furthermore, this study compared performances between conventional NGFWs and a 5G IPS system with the scheme employed, to ascertain that the scheme is feasibly implementable in 5G SA network. The actual test results show a detection rate of 99.7% and reasonable resource overhead (Memory usage 37.8%, CPU usage 42-44%).

INDEX TERMS Mobile network security, availability attacks, confidentiality attacks, integrity attacks, authentication attacks, impersonation attacks, intrusion prevention system, intrusion detection, next generation firewall, signaling attacks, spoofing attacks, flooding attacks.

I. INTRODUCTION

5G standard is divided into two modes—5G Non-Standalone (NSA) and 5G Standalone (SA). The former is 5G core network that permits 4G Long Term Evolution (LTE) core network to coexist, which was first launched by Korea in April, 2019 [1], and is currently used worldwide. Meanwhile, the latter is 5G-only new core network, which was initiated by the US in August, 2020, and is commercially serviced, as of June, 2021, by 12 mobile network operators across 9 countries worldwide [2]. 5G SA is still underway for commercialization along with development for advanced architecture, where research on security technologies is indispensable for provision of stable 5G SA services. In particular, since 5G will be used for medical services that provide a very short delay time and require immediate response, interference from

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

the attacker can be related to our lives. Eventually, the role of the security system in the 5G network becomes more important, and this is acting as a strong motivation for us to conduct this study. Vulnerabilities if found in 5G core network are tackled with patches released by system vendors. However, there are cases in which the vulnerability cannot be fixed with such patches depending upon the on-premise environment of 5G core network. Vulnerabilities that can be corrected via operating system patching encompass those triggered by bugs or flaws of the system per se and those caused by imperfect standards requiring system modification and update [3]–[5]. On the other hand, vulnerabilities hardly correctable via system patching include those often failing to be patched when product vendor patches are not enforced in place or security considerations are insufficient in standards [6]–[11]. Options for tackling non-correctable vulnerabilities via system patching might be to procure and operate an additional security system alongside core network systems, where such system can be used to respond to vulnerability disclosures during the window of vulnerability prior to release of patches by vendors of core network systems. In mobile networks, tremendous traffic created by numerous mobile users are carried by diverse cellular systems and protocols in core networks. Therefore, 5G security systems are required, in addition to security features, to collect packets transmitted through diverse routes as a basic function and to identify and track users from packet data collected.

Representative 5G vulnerability attacks include attacks such as PFCP-in-GTP and IPSec disable attack [12]. These attacks are very complex to detect, and the attacker cannot be identified without integrated session management. However, the 5G core network uses a wide variety of protocols such as NAS, HTTP, PFCP, and GTP. Also, packets of the interface in which each protocol is used are managed with identities that are difficult to identify. Analyzing the relationship of these interfaces in real time is an important key to integrated session management. Also, SA unlike NSA does not send International Mobile Subscriber Identity (IMSI) but sends the encrypted Subscription Concealed Identifier (SUCI) to conceal the user's identity, thereby making it more complex to identify and track users through network traffic.

There have been many studies related to session management in the past, but it is difficult to apply to a 5G SA network using a complex and special protocol [13]. Therefore, this paper proposes the 5G security system for security assurance within 5G core network and in relation thereto carries out evaluation of performances and security features regarding: 1) traffic collecting technology, 2) session management technology and 3) proposed technique.

The main contributions of this paper are summarized as follows:

1) We analyzed the interfaces used in NAS, HTTP, PFCP, and GTP protocols in real time in the 5G core network and presented a method to manage 5G SA user sessions in an integrated manner. The proposed technique defines traffic collection phase and describes a way to create session information for user identification.
2) We proposed an effective detection algorithm for PFCP-in-GTP and IPSec disable attack, which are representative 5G vulnerability attacks.
3) In practice, we verified the performance superiority through the performance test of the security system equipped with the proposed integrated session management method and detection method.

The proposed system with the proposed technique incorporated can surely be utilized to reinforce SA core network security. In particular, the scheme can independently improve on the defenses to address vulnerabilities without waiting for security patches from product vendors. This paper consists of: Chapter II, titled Preliminary, describes 5G SA network architecture and 5G SA registration procedure; relevant researches in Chapter III; Chapter IV presents the proposed technique; Chapter V shows the environment under which the proposed technique is to be validated; the result of the evaluation performed in Chapter VI; Chapter VII presents the content of analysis on the evaluation result; and, Chapter VIII draws a conclusion outlining the outcome of this work.

II. PRELIMINARY

In this chapter we will discuss 5G SA network architecture and 5G SA registration procedure, i.e. the procedure for the User Equipment (UE) registration with the 5G core network.

A. 5G SA NETWORK ARCHITECTURE

The 5G SA core network architecture comprises 26 split network functions (NFs) and entities [14]. Fig. 1 depicts main NFs necessary for user session management, majority of which constitutes 5G network architecture that also corresponds to the scope of this work, Each of these elements is described hereunder.

1) UE (User Equipment)
: A user terminal connected to the mobile core network including ME (Mobile Equipment) and SIM (Subscriber Identity Module), to use network services.
2) gNB (next generation Node B)
: A base station that supports 5G NR (New Radio).

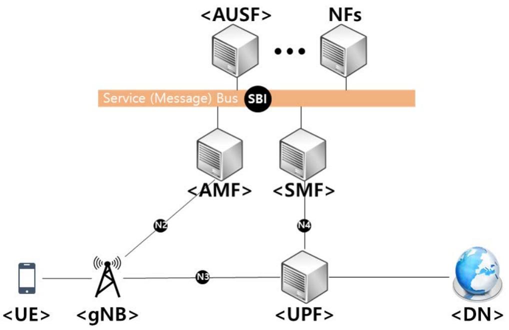


FIGURE 1. 5G SA network architecture.

3) AMF (Access and mobility Management Function)
   : 5G core network function that performs registration, connection, reachability, mobility management, etc.
4) SMF (Session Management Function)
   : 5G core network function that manages subscriber session.
5) AUSF (Authentication Server Function)
   : 5G core network function that supports authentication and security features with respect to UE being connected to 5G core network.
6) UPF (User Plane Function)
   : 5G core network function that supports packet routing/forwarding, interconnect to DN (Data Network), etc. with respect to UE's UP (User Plane) data.
7) DN (Data Network)
   : Refers to the service part outside 5G core network, including Internet and service provider.

B. 5G SA REGISTRATION PROCEDURE

As shown in Figure 2, the 5G SA Registration procedure can largely be divided into two processes, where the one covers from Registration Request to Registration Accept, enabling UEs to register with 5G core network, and the other covers from PDU Session Establishment Request to PDU Session Resource Response, during which an IP address is allocated the session is created. The registration process in 5G SA is different from the 5G NSA Attach process in which IP allocation as well as session creation are made during the registration with the network.

1) 5G AUTHENTICATION AND NAS SECURITY SETUP PROCEDURE

The procedural sequences numbered from 1 to 5 in Fig. 2 are detailed below.

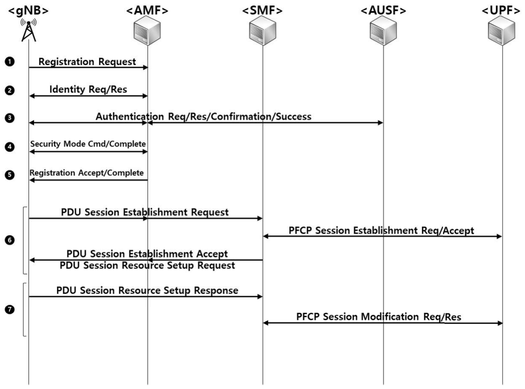

<gNB>
<AMF>
<SMF>
<AUSF>
<UPF>
❶
Registration Request
❷
Identity Req/Res
❸
Authentication Req/Res/Confirmation/Success
❹
Security Mode Cmd/Complete
❺
Registration Accept/Complete
❻
PDU Session Establishment Request
PFCP Session Establishment Req/Accept
PDU Session Establishment Accept
PDU Session Resource Setup Request
❼
PDU Session Resource Setup Response
PFCP Session Modification Req/Res

FIGURE 2. **5G SA registration procedure.**

(a) The UE attempts to gain access to the network through Registration Request message. For an initial registration, reaching the UE is made through SUCI that encrypts Subscriber Permanent Identifier (SUPI) with the UE ID value. If the UE that is in a registered state attempts to gain access again to the network, reaching the UE is made through the old 5G-GUTI mapped from the network during the previous registration procedure.

(b) As the UE identification and authentication process is made through SUCI, if the Registration Request has not been performed through SUCI or if an AMF cannot find SUCI corresponding to 5G-GUTI, the AMF will request SUCI to the UE. This step can be skipped when the AMF can verify SUCI attempting to gain access to the network.

(c) This step relates to authentication of UE and creation of cryptograph key between AMF-UE communication. For the authentication, 5G Authentication and Key Agreement (AKA) or Extensible Authentication Protocol-AKA' (EAP-AKA$'$) may be used by selecting an algorithm the UE and 5G core network support. If SUCI or the UE's SUPI is known by the AMF that received Registration Request message, the Authentication Request is sent to the AUSF through the SUPI. The AUSF gets issued SUPI and Authentication Vector (AV) through Unified Data Management (UDM), and 5G AKA forwards 5G Serving Environment (SE) AV and EAP-AKA$'$ forwards AKA$'$-Challenge to the UE to request for authentication. For the UE, the USIM of the UE verifies the freshness of the AV and authenticates the 5G core network. 5G AKA computes RES$*$, and EAP-AKA$'$ computes RES, and then sends Cipher Key (CK) and Integrity Key (IK) to the ME. RES$*$ and RES are sent to the 5G core network. As for 5G AKA, the verification is made on both AMF and AUSF; as for EAP-AKA$'$, the verification is made on AUSF.

If successfully verified, then the authentication finishes. After the completion of the authentication on AUSF, K_SEAF is forwarded to the AMF. The AMF creates K_AMF and K_ASME, and creates on K_ASME the cipher key and integrity key between AMF-UE, being used for the Non-Access Stratum (NAS) message ciphering.

(d) The step of Security Mode relates to determining ciphering algorithm and integrity algorithm to be used in NAS messages between the UE and the AMF. By referencing to the UE security capability forwarded by the Registration Request, the AMF selects one among algorithms it supports, either being the highest strength of cryptographic algorithm or following the priority set by the network. Then, the AMF sends the Security Mode Command. The UE that received the Security Mode Command applies the corresponding cryptographic algorithm from the rest of NAS messages, whereby all NAS messages from the Security Mode Complete message shall be ciphered and integrity protected.

(e) In this last step for the registration with the network, 5G-GUTI shall be sent to the UE. The gNB creates K_gNB through K_ASME and sends it to be used in UE-gNB Access Stratum (AS) security. The UE that has received 5G-GUTI responds it with the Registration Complete message.

2) 5G PDU SESSION ESTABLISHMENT PROCEDURE

The procedural sequences numbered from 6 to 7 in Fig. 2 are detailed below.

(f) This step relates to sending the PDU Session Establishment Request message including Protocol Data Unit (PDU)

Session ID selected by the UE and whether to support Internet Protocol (IP) v4/v6. The AMF forwards the message to the SMF to create a session on the SMF and sets up diverse rules for the session management of the UE on the UPF. During this process, Uplink tunnel endpoint identifier (TEID) with respect to the UE session is created and is sent, including UPF IP, through the PDU Session Establishment Accept message.

(g) In Next Generation Application Protocol (NAGP) that is the lower layer, PDU Session Resource Setup Request is sent at the time when the PDU Session Establishment Accept message is sent. In response to it, Downlink TEID is created and is sent, including gNB IP, to the PDU Session Resource Setup Response message. Downlink, The gNB IP information shall be updated to the UPF, then the session creation procedure ends.

III. STUDIES OF SECURITY CHALLENGES

GPRS Tunnelling Protocol (GTP) is an important protocol used to allocate UE IP or manage network resources in mobile networks, but it is a UDP-based, disconnected protocol that has a vulnerability that facilitates forgery of packets. A GTP-in-GTP packet refers to a packet containing a GTP-Control (GTP-C) message in a payload corresponding to the user data portion of a GTP-User (GTP-U) packet, and can be easily produced using a packet manipulation tool. In addition, GTP-in-GTP packets can be used to scan the internal equipment of the mobile network or to drain resources of the mobile network [15].

Flooding in a mobile network is an attack that causes a large amount of traffic to occur in the base station or core network systems, making the service disabled. This is mainly in the form of Denial-of-Service (DoS) attacks which are utilized to drain resources on core network systems such as the UPF. In addition, it exists in various forms depending on the target of attack, such as a method of consuming all the bandwidth allowed by the base station. There is no problem in using the system, but increasing network traffic makes mobile services impossible. Small-cell with low capacity can easily be exposed to such attacks, and if attacked, pure connection requests from legitimate users will no longer be possible, making it difficult to provide 5G services [16].

Spoofing attacks are a technique of deceiving identification information to attack other target systems, and appear in the form of disguising and hiding IP addresses, DNS names, and MAC addresses. An attacker on a 5G network is based on a vulnerability in the NAS or SIP protocol. These attacks enable various other attacks, such as packet sniffing, DoS, and session hijacking. Types of spoofing attacks include Mobile Station Integrated System Digital Network (MSISDN) spoofing, IP spoofing, DNS spoofing, etc. [17]

Sniffing refers to collecting and eavesdropping data flowing on a network. In the 5G network, the radio area is the most vulnerable, and sniffing can be performed using fake base stations. Typically, Software Defined Radio (SDR) devices using a USRP may be used to access a fake base station in which nearby terminals are randomly made. All hosts in a area share the same frequency on a base station, so that all traffic communicated by nearby UEs can be seen. However, since the 3GPP standard defines the radio access to be confidential by utilizing multiple cryptographic algorithms, existing papers have dealt with various techniques for breaking encryption, which allows all traffic passing through fake base stations to be intercepted [18].

Ruhr University in Bochum, Germany, first introduced an attack that avoids encryption and integrity checks on NAS messages that have been applied from 4G mobile networks. This can also be valid in 5G networks, which are defined in the 3GPP standard to enable null-encryption and null-integrity in AMF in charge of authentication in 5G core network. However, in the case of integrity, it is a mandatory option. If it is set not to be encrypted, all messages exchanged by the UE are transmitted to the plane-text, thereby infringing confidentiality. Connection using the null-encryption and null-integrity options is allowed due to implementation or device configuration issues, as indicated by M. Closta *et al.* In particular, The "UE Security Capability" value of the Registration message is used to determine AS security. Therefore, if a connection is made after sending the registration message to the null-encryption and null-integrity option in the field, the AS connection will be null-encryption and null-integrity as well. Because AS security is an RAN segment, an attacker can easily capture network traffic from nearby normal UE via sniffing tool such as a fake base station [19]. In addition, many fuzzers have been created in the past, where these attacks are possible on 5G networks. The National Computing Centre (NCC) group which is an information assurance firm to claim over 15,000 clients worldwide in Manchester, UK, introduces three representative things: Fuzzowski 5GC, Frizzer2, and AFLNet. Among them, Frizzer2 and AFLNet are open source network protocol fuzzers that anyone can access [20].

Also, there have been many studies using session management [21], [22]. There have been studies that use metadata such as session generation time, packet size, and packet reception time to generate features at the packet layer and use them for machine learning, or create features at the session layer and use them for machine learning [23]. In particular, studies have been conducted to detect attack traffic by utilizing large-sized payloads occurring at the session layer in machine learning algorithms. However, there has been no research on detecting abnormal traffic through Session Management in 5G networks.

IV. PROPOSED TECHNIQUE FOR SESSION MANAGEMENT

Chap. 4 describes the proposed technique with focus on traffic collection phase and how to collect fields for the session management.

A. SESSION MANAGEMENT TECHNIQUE

1) TRAFFIC COLLECTION PHASE

Fig. 3 depicts traffic collection phases with reference point representation. Phases essentially required for the user

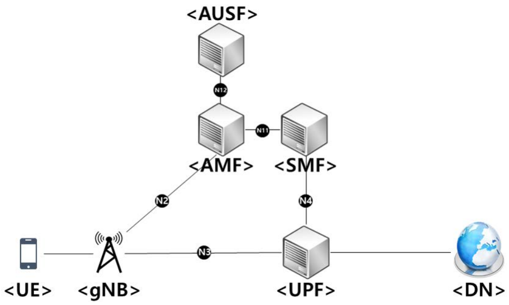
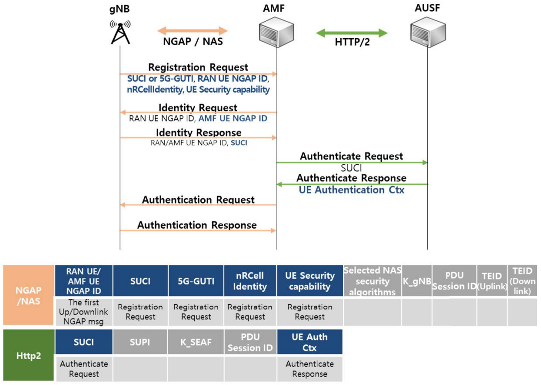


FIGURE 3. 5G Traffic collection phases.

identification and session management are AMF-SMF N11 interface and gNB-UPF N3 interface. Other phases are those added to tackle vulnerabilities targeted on 5G SA core networks. The gNB-AMF N2 interface was added to respond to Null ciphering attack [24], and collecting AMF-AUSF interfaces is also required for deciphering of encrypted NAS phase. The SMF-UPF N4 phase was added to detect Packet Forwarding Control Protocol (PFCP)-in-General Packet Radio Service Tunneling Protocol (GTP) attack, that is, association of GTP-in GTP vulnerability [25] on the SA mode.

2) COLLECTING MAJOR FIELDS ON 5G SA

Fig. 4 and Fig. 5 summarize fields collected for the UE registration procedure with the network, and Fig. 6 and Fig. 7 summarize fields collected for the session creation procedure.

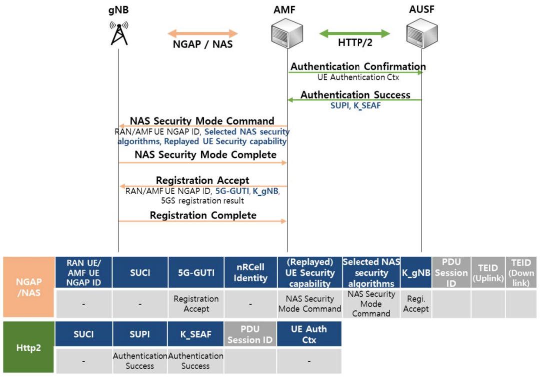


NGAP /NAS	RAN UE/ AMF UE NGAP ID	SUCI	5G-GUTI	nRCell Identity	UE Security capability	Selected NAS security algorithms	K_gNB	PDU Session ID	TEID (Uplink)	TEID (Down link)
	The first Up/Downlink NGAP msg	Registration Request	Registration Request	Registration Request	Registration Request					

Http2	SUCI	SUPI	K_SEAF	PDU Session ID	UE Auth Ctx
	Authenticate Request				Authenticate Response

FIGURE 4. Collected fields for the procedure of UE registration with network (1/2).

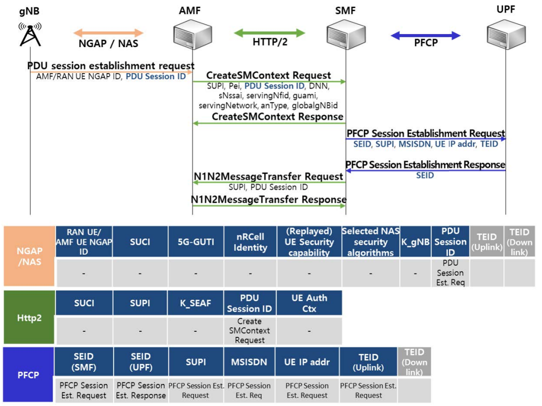
Table 1 outlines collected fields, collected messages and fields for identifying the pertinent messages in a matrix format. As information on N4 phase is also delivered over N11, it is possible to collect major session fields within the N11 phase, if the N4 phase is not needed. The CreateSMContext Request message of the N11 phase extracts PDU Session ID for the identification of user session, and besides can collect as necessary Data Network Name (DNN) and single Network slice selection assistance information (sNssai), etc. that is network slicing information.


gNB
AMF
AUSF
NGAP / NAS
HTTP/2
Authentication Confirmation
UE Authentication Ctx
Authentication Success
SUPI, K_SEAF
NAS Security Mode Command
RAN/AMF UE NGAP ID, Selected NAS security algorithms, Replayed UE Security capability
NAS Security Mode Complete
Registration Accept
RAN/AMF UE NGAP ID, 5G-GUTI, K_gNB, 5GS registration result
Registration Complete

NGAP /NAS	RAN UE/ AMF UE NGAP ID	SUCI	5G-GUTI	nRCell Identity	(Replayed) UE Security capability	Selected NAS security algorithms	K_gNB	PDU Session ID	TEID (Uplink)	TEID (Down link)
	-	-	Registration Accept	-	NAS Security Mode Command	NAS Security Mode Command	Regi. Accept			

Http2	SUCI	SUPI	K_SEAF	PDU Session ID	UE Auth Ctx
	-	Authentication Success	Authentication Success		-

FIGURE 5. Collected fields for the procedure of UE registration with network (2/2).

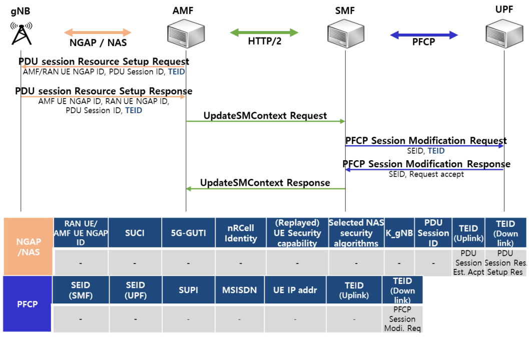

gNB
AMF
SMF
UPF
NGAP / NAS
HTTP/2
PFCP
PDU session establishment request
AMF/RAN UE NGAP ID, PDU Session ID
CreateSMContext Request
SUPI, Pei, PDU Session ID, DNN, sNssai, servingNfid, guami, servingNetwork, anType, globalgNBid
CreateSMContext Response
PFCP Session Establishment Request
SEID, SUPI, MSISDN, UE IP addr, TEID
PFCP Session Establishment Response
SEID
N1N2MessageTransfer Request
SUPI, PDU Session ID
N1N2MessageTransfer Response

NGAP /NAS	RAN UE/ AMF UE NGAP ID	SUCI	5G-GUTI	nRCell Identity	(Replayed) UE Security capability	Selected NAS security algorithms	K_gNB	PDU Session ID	TEID (Uplink)	TEID (Down link)
	-	-	-	-	-	-	-	PDU Session Est. Req		

Http2	SUCI	SUPI	K_SEAF	PDU Session ID	UE Auth Ctx
	-	-	-	Create SMContext Request	-

PFCP	SEID (SMF)	SEID (UPF)	SUPI	MSISDN	UE IP addr	TEID (Uplink)	TEID (Down link)
	PFCP Session Est. Request	PFCP Session Est. Response	PFCP Session Est. Request	PFCP Session Est. Req	PFCP Session Est. Request	PFCP Session Est. Request	

FIGURE 6. Collected fields for the procedure of UE IP allocation and session creation (1/2).


gNB
AMF
SMF
UPF
NGAP / NAS
HTTP/2
PFCP
PDU session Resource Setup Request
AMF/RAN UE NGAP ID, PDU Session ID, TEID
PDU session Resource Setup Response
AMF UE NGAP ID, RAN UE NGAP ID, PDU Session ID, TEID
UpdateSMContext Request
PFCP Session Modification Request
SEID, TEID
PFCP Session Modification Response
SEID, Request accept
UpdateSMContext Response

NGAP /NAS	RAN UE/ AMF UE NGAP ID	SUCI	5G-GUTI	nRCell Identity	(Replayed) UE Security capability	Selected NAS security algorithms	K_gNB	PDU Session ID	TEID (Uplink)	TEID (Down link)
	-	-	-	-	-	-	-	-	PDU Session Est. Acpt	PDU Session Res. Setup Res

PFCP	SEID (SMF)	SEID (UPF)	SUPI	MSISDN	UE IP addr	TEID (Uplink)	TEID (Down link)
	-	-	-	-	-	-	PFCP Session Modi. Req

FIGURE 7. Collected fields for the procedure of UE IP allocation and session creation (2/2).

3) CREATION AND MANAGEMENT OF SESSION MANAGEMENT TABLE

Fig. 8 prunes down a UE session table for the user session identification and a key table for NAS phase deciphering. K_AMF in the key table can be created from collected K_SEAF according to the procedure specified in Annex A.7 of 3GPP TS 33.501 [26], and K_NASint and K_NASenc can be created from K_AMF according to the procedure specified in Annex A.8 of 3GPP TS 33.501 [27]. Created

TABLE 1. Collected fields in messages of 5G standalone.

Collected field	Collected message	Field for identifying collected message	Description
SUPI	N12 Authentication Success	HTTP/2 Stream Identifier of Authentication Confirmation	Subscriber's unique ID
SUCI	N2 Registration Request N12 Authentication Request	N2 : NONE N12 : SUCI	Encrypted SUPI
5G-GUTI	N2 Registration Request	NONE	Subscriber's temporary ID
MSISDN	N4 PFCP Session Establishment Request	SUPI	Mobile Station International Integrated Services Digital Network Number
RAN UE / AMF UE NGAP ID	N2 The first UP/Downlink NGAP message	NONE	AMF-gNB NGAP communication ID
nRCell Identity	N2 Registration Request	SUCI	Global unique gNB ID
UE Security Capability	N2 Registration Request N2 NAS Security Mode Command (Replayed)	SUCI Replayed : RAN/AMF UE NGAP ID	Encryption and integrity algorithm that UE supports
Selected NAS Security Algorithm	N2 NAS Security Mode Command	RAN/AMF UE NGAP ID	Encryption and integrity algorithm selected by core network
SEID	N4 PFCP Session Establishment Request/Response	Request : SUPI Response: Sequence number of Request message	SMF-UPF tunnel ID
TEID	N2 PDU Session Establishment Accept N2 PDU Session Resource Setup Response N4 PFCP Session Establishment Request N4 PFCP Session Modification Request	N2 : RAN/AMF UE NGAP ID N4 : SUPI, TEID	gNB-UPF Tunnel ID
PDU Session ID	N2 PDU Session Establishment Request N11 CreateSMContext Requets	N2 : RAN/AMF UE NGAP ID N4 : SUPI	UE's session ID
UE IP address	N4 PFCP Session Establishment Request	SUPI	UE's session IP address
UE Authentication Ctx	N12 Authenticate Response	HTTP/2 Stream Identifier of Authentication Request	Authentication Context (location)
K_SEAF	N12 Authentication Success	HTTP/2 Stream Identifier of Authentication Confirmation	Used to create K_AMF with Security Anchor Function Key
K_gNB	N2 Registration Accept	RAN/AMF UE NGAP ID	Used to create AS security key with gNB Key

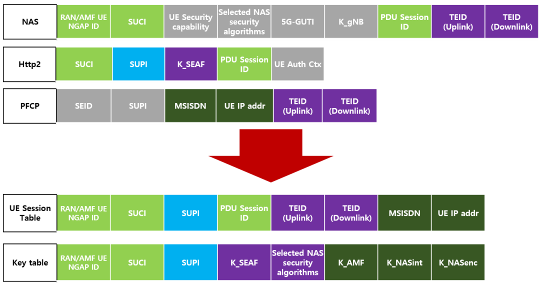


FIGURE 8. Creation of session management table.

session tables need to be modified or deleted in the event of PFCP Modification and PFCP Deletion messages where Session Endpoint Identifier (SEID) and TEID coincide.

B. DETECTION EXAMPLES

1) PFCP-IN-GTP ATTACK

The PFCP-in-GTP attack is shown in Fig. 9. Security features of the proposed system were validated by testing 2 vulnerabilities exploitable in 5G SA network [11]–[27]. The first vulnerability involves detection algorithm against PFCP-in-GTP attack. This type of attack is accomplished such that PFCP protocol message used only in the 5G core network is injected into data the user transmits and sent to the targeted UE. If successful, the attacker can plug into the 5G core network system to issue its arbitrary command.

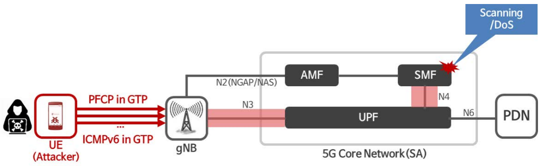


FIGURE 9. Procedure of PFCP in GTP attack.

A security system to counteract such type of attack must inspect and block the injected packet at the front door of the core network from a security standpoint. The detection algorithm mentioned above checks if the PFCP header exists in payload of GTP-U packet through Deep Packet Inspection (DPI). In this algorithm, input data is when port 2152 is used among uplink packets passing UPF, and output data is detection information of PFCP-in-GTP attack including attacker's identification factors (IMSI, IP, etc.) when detected.

Fig. 10 is a PFCP-in-GTP attack detection algorithm that goes through a total of three procedures. The first checks whether the packet entering the detection system is a GTP-U protocol. GTP-U has a port fixed at 2152 according to the 3GPP TS 29.281 defined for the GPRS tunneling protocol. Therefore, it checks whether the destination port of the packet is 2152. Second, the payload of the packet must be checked. In general, the user data packet is TCP or UDP, and the detection algorithm should find a case of UDP and PFCP. PFCP has a port fixed at 8805 in accordance with the 3GPP TS

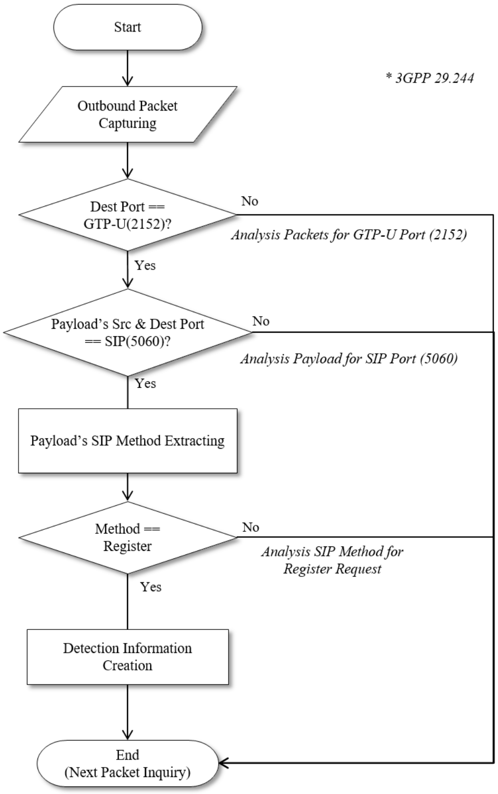

Start
Outbound Packet Capturing
* 3GPP 29.244
Dest Port == GTP-U(2152)?
No
Analysis Packets for GTP-U Port (2152)
Yes
Payload's Src & Dest Port == SIP(5060)?
No
Analysis Payload for SIP Port (5060)
Yes
Payload's SIP Method Extracting
Method == Register
No
Analysis SIP Method for Register Request
Yes
Detection Information Creation
End (Next Packet Inquiry)

FIGURE 10. PFCP in GTP attack detection algorithm.

29.244 that defines the interface between the Control Plane and the User Plane. Therefore, the algorithm checks whether the UDP port of the payload in the packet is 8805. Third, it is possible to know the type of attack depending on which message among PFCPs is used. Extracting the top 4 bytes results in a message type, for example, 0 × 2*32 (where "*" may contain a value of 0 or 1 depending on whether or not the endpoint of the entity sending the message) as a PFCP Session Estimation Request, requesting the creation of a session between SMF and UPF. If the detected packet contains the corresponding PFCP message, it is a request to create a false session and can intentionally consume session resources through repeated attacks.

2) SIP IPSec DISABLE ATTACK

The second vulnerability involves detection algorithm against SIP malformed attack. This type of attack can make the system unstable, such as eavesdropping, by arbitrarily disabling the user's use of IPSec that encrypts packets of data. The SIP IPSec disable attack is shown in Fig. 11.

A security system to counteract such type of attack must inspect and block the SIP Register packets at the front door of CSCF that is a SIP server. The detection algorithm mentioned above checks if the use of IPSec is disabled, by grouping records as to normal SIP Register messages to Reference Packet Group (RPG) and comparing Experimental Packet Group (EPG) with the RPG. In this algorithm, input data is when port 2152 is used among uplink packets passing UPF, and output data is detection information of SIP IPSec disable attack including attacker's identification factors (IMSI, MSISDN, etc.) when detected.

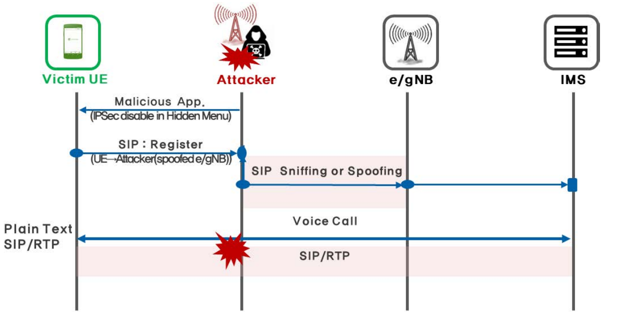


FIGURE 11. Procedure of SIP IPSec disable attack.

Fig. 12 is a IPSec disable attack detection algorithm that goes through a total of four procedures. The first checks whether the packet entering the detection system is a GTP-U protocol. As mentioned in the previous chapter, the port is fixed at 2152. Therefore, it checks whether the destination port of the packet is 2152. Second, the payload of the packet must be checked. In general, since the voice service packet used in the 5G network is SIP, it is necessary to find a case in which the detection algorithm is UDP and SIP. The port of

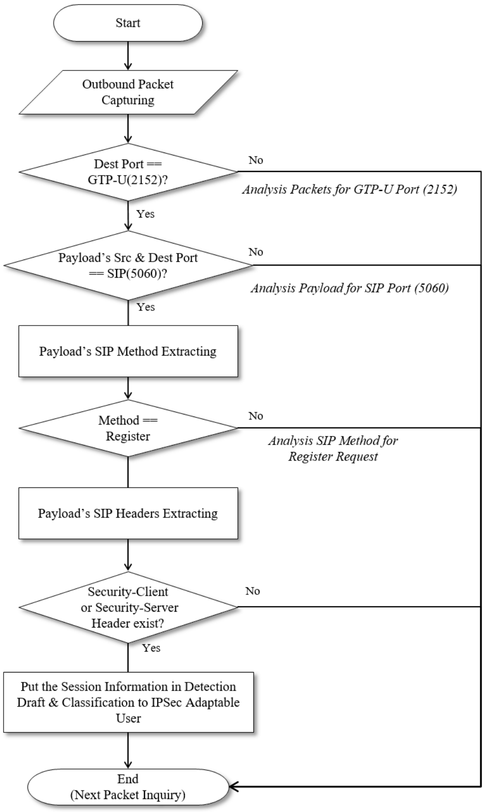

Start
Outbound Packet Capturing
Dest Port == GTP-U(2152)?
No
Analysis Packets for GTP-U Port (2152)
Yes
Payload's Src & Dest Port == SIP(5060)?
No
Analysis Payload for SIP Port (5060)
Yes
Payload's SIP Method Extracting
Method == Register
No
Analysis SIP Method for Register Request
Payload's SIP Headers Extracting
Security-Client or Security-Server Header exist?
No
Yes
Put the Session Information in Detection Draft & Classification to IPSec Adaptable User
End (Next Packet Inquiry)

FIGURE 12. SIP IPSec disable attack detection algorithm.

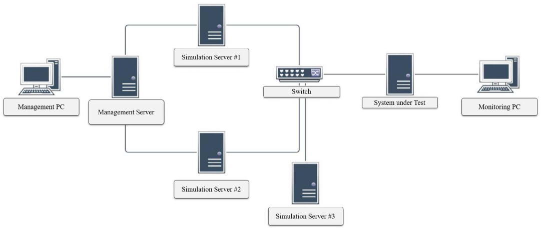


FIGURE 13. Physical environment.

the SIP is fixed at 5060 according to the RFP3261 standard. Accordingly, the UDP port of the payload in the packet uses 5060. Third, the algorithm should find a message in SIP where the method value is Register and request. A register request is a message in which a UE wishing to use a voice service registers with an IP Multimedia Subsystem (IMS) network that controls the voice service. Finally, it checks whether the SIP header in the Register message contains the Security-Client or Security-Server header. If the SIP Register Request packet contains those headers, this is the case of requesting SIP encryption, and if there is no such header, the UE does not use SIP encryption. If the proposed Session Management Technique is used in the detection system, the SIP encryption request record of the UEs may be recorded. If a user who has previously used encryption requests a register without an encryption-related SIP header, this can be suspected as a change in the UE or a SIP IPSec disable attack. If a UE is changed, a device that uses SIP encryption is white-listed for each UE, and if there is no encryption-related SIP header in the register message, the 5G network security operator needs to upgrade from the suspected SIP IPSec disable attack to the dangerous level. In this case, the security operator needs to monitor voice call traffic for the user and warn the user that the current call is not encrypted.

V. EVALUATION ENVIRONMENT

The evaluation environment will be described by dividing it into three parts. That is, Part A pertains to the experimental architecture for the evaluation, Part B pertains to 5G security threats and test case for security testing, and Part C pertains to metric, reference group and test case for performance testing.

A. EXPERIMENT ARCHITECTURE FOR EVALUATION

The proposed 5G security system was tested under the environments physically as shown in Fig. 9 and logically as shown in Fig. 10. In addition, the control-plane and the user-plane were separated by configuring VLAN as shown in Fig. xx. Furthermore, a 5G core network system simulator (traffic generator) was built making it possible to monitor packets over a total of 4 interfaces composed of N2 interface (b/w gNB and AMF), N3 interface (b/w gNB and UPF), N4 interface (b/w SMF and UPF) and N11 interface (b/w SMF and AMF). The 5G core network system simulator used is Spirent Landslide C100-M4.

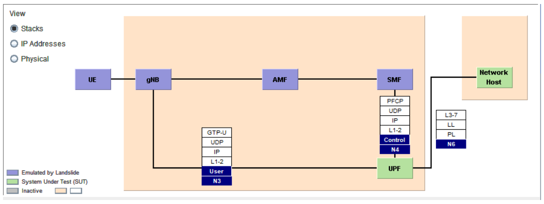


FIGURE 14. Logical environment.

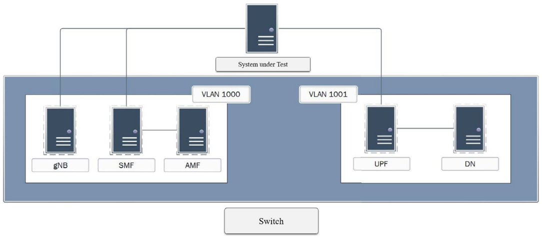
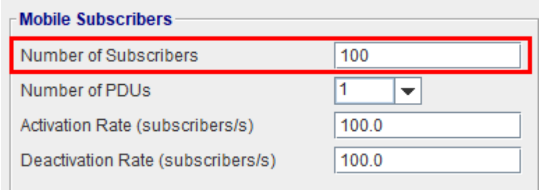


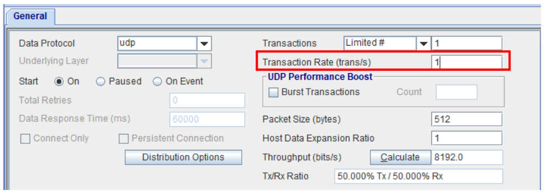
FIGURE 15. Switch VLAN settings.



Mobile Subscribers

Number of Subscribers	100
Number of PDUs	1
Activation Rate (subscribers/s)	100.0
Deactivation Rate (subscribers/s)	100.0

FIGURE 16. Subscribers configuration for detection test.



General

Data Protocol	udp
Underlying Layer	
Start	● On ○ Paused ○ On Event
Total Retries	0
Data Response Time (ms)	60000
□ Connect Only	□ Persistent Connection
Transactions	Limited # 1
Transaction Rate (trans/s)	1
UDP Performance Boost	□ Burst Transactions Count
Packet Size (bytes)	512
Host Data Expansion Ratio	1
Throughput (bits/s)	8192.0
Tx/Rx Ratio	50.000% Tx / 50.000% Rx

FIGURE 17. Transaction rate configuration for detection test.

TABLE 2. Specification of system under test.

Cat.	Specification
CPU	Intel Xeon E5-2640 v4 @2.40 GHz
Memory	62 GB
HDD	1.5 TB
OS	Linux Based Custom OS (Linux Kernel 3.0.13_k3.10.0)
NIC	Intel Corporation WINS WXGEN Fiber (1600) (rev 01) * 2 ports

The test system used hardware specification as shown in Table 2.

B. DETECTION TEST ENVIRONMENT

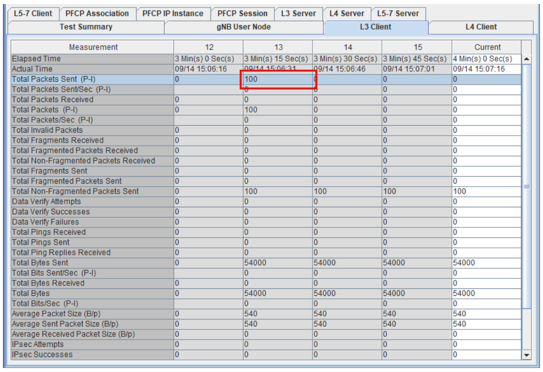
The testing hereof was made after, as for each traffic scenario, setting the Number of Subscribers field to 100 persons, normal packets to UDP, and Transaction Rate to 1.

1) PFCP-IN-GTP ATTACK DETECTION TEST CASES

To reproduce the security scenario for PFCP-in-GTP attack, 8 types in total of payload data of abnormal packets were

TABLE 3. Injected packets for PFCP-in-GTP attack.

No.	Injected Packets	4bytes	Threat
1	Heartbeat Request	0x2*01	SBA Entity Scanning
2	Heartbeat Response	0x2*02	SBA Entity Scanning
3	Session Establishment Request	0x2*32	Session Depletion
4	Session Establishment Response	0x2*33	Session Depletion
5	Session Modification Request	0x2*34	Deny of Service
6	Session Modification Response	0x2*35	Deny of Service
7	Session Deletion Request	0x2*36	Deny of Service
8	Session Deletion Response	0x2*37	Deny of Service



Measurement	12	13	14	15	Current
Elapsed Time	3 Min(s) 0 Sec(s)	3 Min(s) 15 Sec(s)	3 Min(s) 30 Sec(s)	3 Min(s) 45 Sec(s)	4 Min(s) 0 Sec(s)
Actual Time	09/14 15:06:16	09/14 15:06:31	09/14 15:06:46	09/14 15:07:01	09/14 15:07:16
Total Packets Sent (P-I)	0	100	0	0	0
Total Packets Sent/Sec (P-I)		0	0	0	0
Total Packets Received	0	0	0	0	0
Total Packets (P-I)	0	100	0	0	0
Total Packets/Sec (P-I)		0	0	0	0
Total Invalid Packets	0	0	0	0	0
Total Fragments Received	0	0	0	0	0
Total Fragmented Packets Received	0	0	0	0	0
Total Non-Fragmented Packets Received	0	0	0	0	0
Total Fragments Sent	0	0	0	0	0
Total Fragmented Packets Sent	0	0	0	0	0
Total Non-Fragmented Packets Sent	0	100	100	100	100
Data Verify Attempts	0	0	0	0	0
Data Verify Successes	0	0	0	0	0
Data Verify Failures	0	0	0	0	0
Total Pings Received	0	0	0	0	0
Total Pings Sent	0	0	0	0	0
Total Ping Replies Received	0	0	0	0	0
Total Bytes Sent	0	54000	54000	54000	54000
Total Bits Sent/Sec (P-I)		0	0	0	0
Total Bytes Received	0	0	0	0	0
Total Bytes	0	54000	54000	54000	54000
Total Bits/Sec (P-I)		0	0	0	0
Average Packet Size (B/p)	0	540	540	540	540
Average Sent Packet Size (B/p)	0	540	540	540	540
Average Received Packet Size (B/p)	0	0	0	0	0
IPsec Attempts	0	0	0	0	0
IPsec Successes	0	0	0	0	0

FIGURE 18. Sent packet statistics for PFCP-in-GTP attack in traffic generator.

created, for which 100 packets by each type were prefabricated in advance into one PCAP file. Spirent's Landslide STC-C1 package was used as the test case simulator. Table 3 classifies the types of attacks for each PFCP message included in the detected packet.

2) SIP IPSec DISABLED ATTACK DETECTION TEST CASES

SIP message packets with IPSec applied and SIP message packets with IPSec not applied were individually created, and, to transmit test cases to the proposed 5G security system, "a_ipsec = rdpcap" and "a_no_ipsec = rdpcap" were set up in the SIP message packet transmission tool. The SIP headers for IPSec association are shown in Table 4.

TABLE 4. SIP headers for IPSec association.

No.	SIP Headers	Values
1	security-client	"Security-Client" HCOLON sec-mechanism *(COMMA sec-mechanism)
2	security-server	"Security-Server" HCOLON sec-mechanism *(COMMA sec-mechanism)
3	security-verify	"Security-Verify" HCOLON sec-mechanism *(COMMA sec-mechanism)

C. PERFORMANCE TEST ENVIRONMENT

1) METRIC OF PERFORMANCE

NSS Labs published the NGFW Performance Report in 2018, which considered four criteria that affect the device's overall performance. Hereunder is description about these factors, i.e. (a) UDP Throughput, (b) UDP Latency, (c) TCP Connection, and (d) HTTP Connection.

a: UDP LATENCY

Latency expresses the time taken to delivery data packet from one point to another point. The purpose of this test is to measure the device's raw packet processing capability as well as its efficacy at fast forwarding packets in order to provide the best network performance with the least amount of latency. Legacy firewalls have long been thought to be required to give the best level of network speed with the least amount of latency, but because of the DPI that NGFW devices are expected to perform, it has frequently caused significant problems. In-line security devices that introduce high levels of latency lead to poor service quality to users as well as unacceptable packet delay for operators, particularly where they are placed in the data packet transmission path. Throughput tests demonstrate the delay (in μs) at 90% of maximum capacity, with lower values desired. The UDP packet size used is 1514byte.

b: UDP THROUGHPUT

Throughput refers to the maximum amount of successful message delivery per unit time that can be processed by a system. For the measurement thereof, UDP packets of varying sizes generated by the Packet Generator Appliance are used. In the NSS performance assessment report, UDP packets use 6 sizes consisting of 64bytes, 128bytes, 256bytes, 512bytes, 1024bytes and 1514bytes. A steady stream of the proper packet size is sent bidirectionally across each Packet Generator Appliance port pair, together with varying source and destination IP addresses. And, each packet contains dummy data and is directed to a valid port on a valid subnet IP address. Before each test, network monitoring tools verify the percentage load and frames per second (fps) data across each inline port pair. Furthermore, many tests for correctness are performed, and averages are calculated. The test result shows maximum UDP Throughput (Mbps) achievable when each device uses varying packet sizes.

c: MAX TCP CPS(CONCURRENT TCP CONNECTION)

Maximum TCP CPS refers to the maximum number of TCP Connection that can be created per second. The purpose of this test is to put the System under Test (SUT) engine to the test and see how well it handles large numbers of TCP connections per second. The use of Packet Generator Appliance enables an engineer to create traffic at varying Gbps rates as the background load in testing. At various connection/transaction rates, these tests provide a good simulation of a live network because all packets contain valid payload and address data.

All tests use the key Breaking Point which is where the final measurements are taken. (1) Concurrent TCP connections in excess, (2) Excessive con-current HTTP connection, (3) Unsuccessful HTTP transaction (usually, 0 transaction). Connection Rates, in addition to overall throughput, are critical in sizing a security device that won't stifle a system's or application's performance. A device can be scaled more precisely by evaluating Maximum Connection rates rather than only looking at throughput. Once the maximum CPS of a device is established, it is possible to anticipate its maximum throughput depending on the traffic mix in an enterprise setting. If the maximum TCP CPS on the device is 2000 and the average traffic size is 44kb (2500cps = 1Gbps), the device can be considered to have a maximum capacity of 800Mbps, which is (2000/2500)*1000Mbps = 800Mbps by arithmetic.

When attempting to size a device appropriately, maximum concurrent TCP connections and maximum TCP CPS rates are also useful. Low Connection/Throughput ratio products risk depleting connections before reaching their optimum throughput capabilities. It is also possible to forecast when a device may fail in a specific organizational context by knowing the maximum CPS of a system in operation.

d: MAX HTTP CPS(CONCURRENT HTTP CONNECTION)

The HTTP capacity tests are used to determine how effectively the HTTP detection engine manages network loads with varied average packet sizes and connections per second. Because the device is compelled to track genuine HTTP sessions by using traffic with different session lengths, it has a higher effort than if it were just dealing with packets. This simulates real-world situations as closely as possible while assuring precise precision and repeatability. Each transaction is made up of a single HTTP GET request, with valid payload (a combination of binary and ASCII objects) and address data in each packet. This simulation is a great portrayal of a real-time network at various network loads. The greatest performance attained across a range of different HTTP response sizes is shown in the test result. It also shows the maximum APL connection rates (HTTP Connections per second) attained with various HTTP response sizes (from 44kb up to 1.7kb).

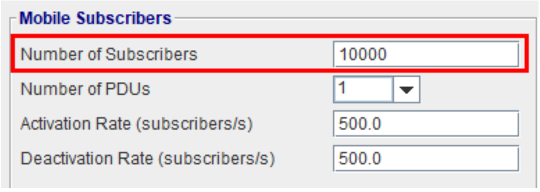
2) COMMERCIALIZED PRODUCTS

Security systems for mobile telecom networks already exist as commercialized products. Some of them are Next Generation Firewall (NGFW) products for packet analysis as to protocol used in existing LTE networks. Typical products are Check Point 15600 NGTP, Cisco Firepower4120, Forcepoint NGFW 2105, Fortinet FortiGate 500E, Palo Alto Networks PA-5220,etc. These appliances include features such as GTP using it in 5G LTE network, diameter protocol using it in DDoS and feature capable of identifying abnormal packets. Of those products, however, there is almost nothing that can be used in 5G network. Therefore, comparative test devices for the purpose of this paper are limited to the context of LTE NGFWs.

3) PERFORMANCE TEST CONFIGURATION

a: LATENCY TEST

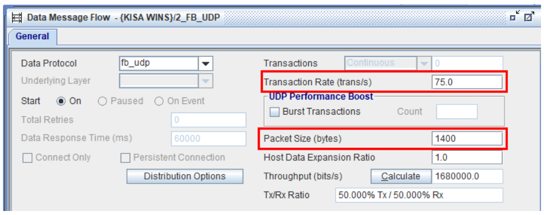
For each traffic scenario, latency testing was performed by setting the number of subscribers to 10,000, UDP packet size to 1400byte, and Transaction Rate to 75.



Mobile Subscribers

Number of Subscribers	10000
Number of PDUs	1
Activation Rate (subscribers/s)	500.0
Deactivation Rate (subscribers/s)	500.0

FIGURE 19. Subscribers configuration for latency test.

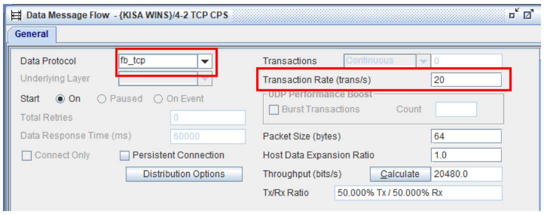


Data Message Flow - {KISA WINS}/2_FB_UDP

General

Data Protocol	fb_udp	Transactions	Continuous 0
Underlying Layer		Transaction Rate (trans/s)	75.0
Start	● On ○ Paused ○ On Event	UDP Performance Boost	□ Burst Transactions Count
Total Retries	0	Packet Size (bytes)	1400
Data Response Time (ms)	60000	Host Data Expansion Ratio	1.0
□ Connect Only	□ Persistent Connection	Throughput (bits/s)	1680000.0
	Distribution Options	Tx/Rx Ratio	50.000% Tx / 50.000% Rx

FIGURE 20. Transaction rate configuration for latency test.



Data Message Flow - {KISA WINS}/4-2 TCP CPS

General

Data Protocol	fb_tcp	Transactions	Continuous 0
Underlying Layer		Transaction Rate (trans/s)	20
Start	● On ○ Paused ○ On Event	UDP Performance Boost	□ Burst Transactions Count
Total Retries	0	Packet Size (bytes)	64
Data Response Time (ms)	60000	Host Data Expansion Ratio	1.0
□ Connect Only	□ Persistent Connection	Throughput (bits/s)	20480.0
	Distribution Options	Tx/Rx Ratio	50.000% Tx / 50.000% Rx

FIGURE 21. Transaction rate configuration for max capacity test.

b: UDP THROUGHPUT TEST

As identical to performance testing of NSS Labs, a variety of UDP packets were used. UDP packet sizes used are 6 types consisting of 64byte, 128byte, 256byte, 512byte, 1024byte, and 1514byte, and the test was made by setting to RFC-2544 of STC.

c: MAX CAPACITY TEST

This test was made such that, for each traffic scenario, the number of subscribers is set to 10000 persons and connection rate is set to create maximum TCP Connections of between 20 and 50 per second. Therefore, measuring the performance was undertaken in an environment of sending/receiving 200,000 to 500,000 TCP SYNs ACKs per second.

VI. EVALUATION RESULTS

A. SESSION MANAGEMENT AND DETECTION TEST

1) PFCP-IN-GTP ATTACK DETECTION TEST

The detection test results of the proposed system for PFCP-in-GTP attacks are shown in Table 5. Assuming that packets of 100 normal subscribers and 8 malicious subscribers send attacks, three tests showed that 100 packets were normal in all three times and 8 abnormal packets were detected.

TABLE 5. PFCP-IN-GTP attack dection test results.

Test No.	TP	FN	TN	FP
1	100	0	8	0
2	100	0	8	0
3	100	0	8	0
Average	100	0	8	0

2) SIP IPSEC DISABLE ATTACK DETECTION TEST

The test result as to the proposed system's capability to detect SIP IPSec Disable attack is given in Table 6. Resulting from three tests by transmitting 100 normal packets and 12 abnormal packets, it was found that in each of all three tests 100 packets are judged as normal and a total of 13 packets including 12 abnormal packets are detected, addressing that there occurs false detection.

TABLE 6. SIP IPSec disable attack detection test results.

Test No.	TP	FN	TN	FP
1	100	0	12	0
2	100	0	12	0
3	99	0	12	0
Average	99.7	0.3	12	0

3) DETECTION TEST RESULT

The detection test result revealed that the proposed system was also able to identify the attacker with maximum detection capacity of at least 99% when using the session management technique. However, there was false detection case when detecting SIP IPSec disable attack, so an attempt was made to check errors in given algorithms. Only the SIP header in the SIP Request was supposed to be determined, but this requires algorithm supplementation to look at the SIP header in the SIP Response together. Exceptionally, the terminal requests IPSec Association, but in some cases, the IMS network does not support it. Therefore, the detection system should check the SIP Response from the network to distinguish if IPSec is not used.

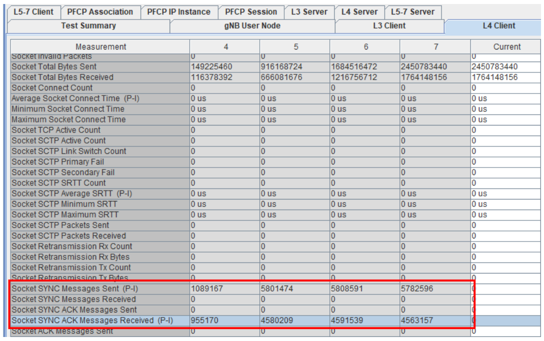
B. PERFORMANCE TEST

1) UDP LATENCY

The UDP latency test results of the proposed system are shown in Table 7. To accurately measure latency time span of the proposed 5G security system, latency introduced by a switch existing in the test environment was measured at the system's maximum load of 90% to measure latency of the equipment under test by subtracting the switch latency time from the total latency time. As the measurement indicates round-trip UDP latency taken until the response packet is arrived as to the request packet in the in-line configuration, final UDP latency can be deemed as a half of the measured latency.

TABLE 7. UDP latency for proposed system.

Test No.	Packet Size	UDP Latency
1	128-bytes	29.72us
2	256-bytes	24.04us
3	512-bytes	23.31us
4	1024-bytes	23.02us
5	1280-bytes	23.35us
6	1514-bytes	23.68us
Average		24.52us



Measurement	4	5	6	7	Current
Socket Invalid Packets	0	0	0	0	0
Socket Total Bytes Sent	149225460	916168724	1684516472	2450783440	2450783440
Socket Total Bytes Received	116378392	666081676	1216756712	1764148156	1764148156
Socket Connect Count	0	0	0	0	0
Average Socket Connect Time (P-I)	0 us	0 us	0 us	0 us	0 us
Minimum Socket Connect Time	0 us	0 us	0 us	0 us	0 us
Maximum Socket Connect Time	0 us	0 us	0 us	0 us	0 us
Socket TCP Active Count	0	0	0	0	0
Socket SCTP Active Count	0	0	0	0	0
Socket SCTP Link Switch Count	0	0	0	0	0
Socket SCTP Primary Fail	0	0	0	0	0
Socket SCTP Secondary Fail	0	0	0	0	0
Socket SCTP SRTT Count	0	0	0	0	0
Socket SCTP Average SRTT (P-I)	0 us	0 us	0 us	0 us	0 us
Socket SCTP Minimum SRTT	0 us	0 us	0 us	0 us	0 us
Socket SCTP Maximum SRTT	0 us	0 us	0 us	0 us	0 us
Socket SCTP Packets Sent	0	0	0	0	0
Socket SCTP Packets Received	0	0	0	0	0
Socket Retransmission Rx Count	0	0	0	0	0
Socket Retransmission Rx Bytes	0	0	0	0	0
Socket Retransmission Tx Count	0	0	0	0	0
Socket Retransmission Tx Bytes	0	0	0	0	0
Socket SYNC Messages Sent (P-I)	1089167	5801474	5808591	5782596	0
Socket SYNC Messages Received	0	0	0	0	0
Socket SYNC ACK Messages Sent	0	0	0	0	0
Socket SYNC ACK Messages Received (P-I)	955170	4580209	4591539	4563157	0
Socket ACK Messages Sent	0	0	0	0	0

FIGURE 22. TCP connection statistics in traffic generator.

2) UDP THROUGHPUT

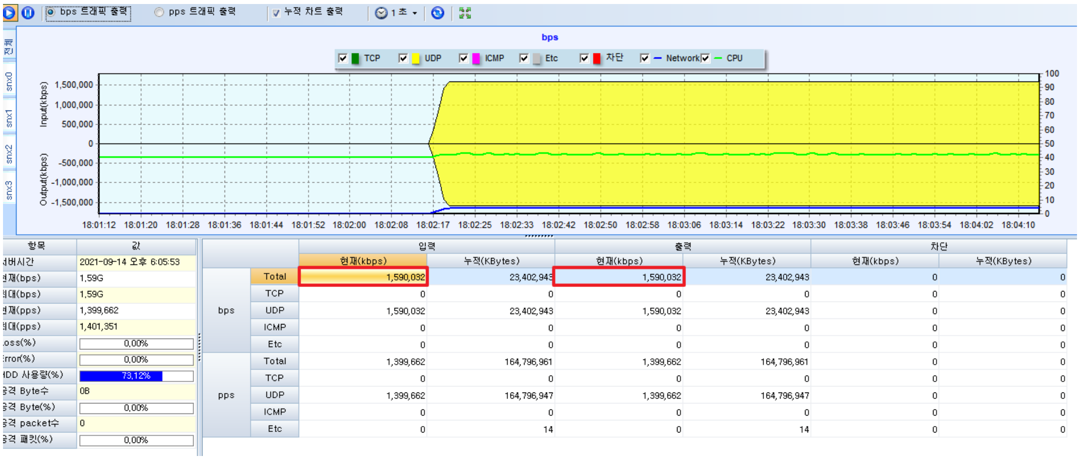
The UDP throughput test results of the proposed system are shown in Table 8. As identical to performance testing of NSS Labs, a variety of UDP packets were used. Note, however, that the minimum size of UDP packet must be at least 86bytes because of encapsulation to GTP protocol given characteristic features of the mobile communication packet. Therefore, tests were performed in the condition of 128bytes, 256bytes, 512bytes, 1024bytes, 1280bytes and 1514bytes, respectively, where maximum throughput was 20Gbps. As for UDP throughput, its performance can be enhanced by way of changing hardware as it is dependent upon performance of network card mounted in the system.

TABLE 8. UDP throughput for proposed system.

Test No.	Packet Size	Throughput
1	128-bytes	18.2Gbps
2	256-bytes	19.5Gbps
3	512-bytes	20Gbps
4	1024-bytes	20Gbps
5	1280-bytes	20Gbps
6	1514-bytes	20Gbps
Average		19.62Gbps

3) MAX CAPACITY (TCP/HTTP CPS)

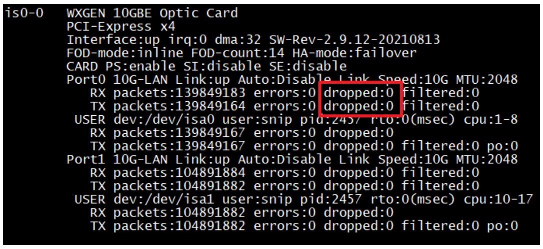
Measuring volumes of TCP Connections per second and loss of any Connection message was conducted by checking statistical data of the simulator and checking the network card interface information on the monitoring screen of SUT. TCP CPS (Socket SYNC Messages Sent (P-I) and Socket ACK Messages Received (P-I)) shown in Fig. 22 is the statistical values for 15 seconds. Therefore, to calculate TCP CPS, it is required to divide Socket SYNC Messages Sent (P-I) or Socket ACK Messages Received (P-I) by 15 seconds. For



항목	값
버시간	2021-09-14 오후 6:05:53
재(bps)	1,59G
대(bps)	1,59G
재(pps)	1,399,662
대(pps)	1,401,351
oss(%)	0,00%
rror(%)	0,00%
DD 사용량(%)	73,12%
격 Byte수	0B
격 Byte(%)	0,00%
격 packet수	0
격 패킷(%)	0,00%

		입력		출력		차단	
		현재(kbps)	누적(KBytes)	현재(kbps)	누적(KBytes)	현재(kbps)	누적(KBytes)
bps	Total	1,590,032	23,402,943	1,590,032	23,402,943	0	0
	TCP	0	0	0	0	0	0
	UDP	1,590,032	23,402,943	1,590,032	23,402,943	0	0
	ICMP	0	0	0	0	0	0
	Etc	0	0	0	0	0	0
pps	Total	1,399,662	164,796,961	1,399,662	164,796,961	0	0
	TCP	0	0	0	0	0	0
	UDP	1,399,662	164,796,947	1,399,662	164,796,947	0	0
	ICMP	0	0	0	0	0	0
	Etc	0	14	0	14	0	0

FIGURE 23. TCP connection statistics in proposed system.



```
is0-0    WXGEN 10GBE Optic Card
         PCI-Express x4
         Interface:up irq:0 dma:32 SW-Rev-2.9.12-20210813
         FOD-mode:inline FOD-count:14 HA-mode:failover
         CARD PS:enable SI:disable SE:disable
         Port0 10G-LAN Link:up Auto:Disable Link Speed:10G MTU:2048
            RX packets:139849183 errors:0 dropped:0 filtered:0
            TX packets:139849164 errors:0 dropped:0 filtered:0
          USER dev:/dev/isa0 user:snip pid:2457 rto:0(msec) cpu:1-8
            RX packets:139849167 errors:0 dropped:0
            TX packets:139849167 errors:0 dropped:0 filtered:0 po:0
         Port1 10G-LAN Link:up Auto:Disable Link Speed:10G MTU:2048
            RX packets:104891884 errors:0 dropped:0 filtered:0
            TX packets:104891882 errors:0 dropped:0 filtered:0
          USER dev:/dev/isa1 user:snip pid:2457 rto:0(msec) cpu:10-17
            RX packets:104891882 errors:0 dropped:0
            TX packets:104891882 errors:0 dropped:0 filtered:0 po:0
```

FIGURE 24. Dropped packet statistics in proposed system.

example, by dividing 3,000,000 by 15 seconds, 200,000 CPS is obtained. In this test, the Request message size for TCP Connection was 151 bytes, and the Response message size was 266 bytes.

The Max capacity test results of the proposed system are shown in Table 9 and 10. Resulting from three tests in total, it was found that loss of TCP Connection happened from 400,000 CPS for the second test, and from 450,000 CPS for the first and third tests.

TABLE 9. TCP CPS for proposed system.

Test No.	TCP CPS with Dropped Connection	Max TCP CPS
1	450,000 CPS	400,000 CPS
2	400,000 CPS	350,000 CPS
3	450,000 CPS	400,000 CPS
Average		383,333 CPS

TABLE 10. HTTP CPS for proposed system.

Test No.	HTTP CPS with Dropped Connection	Max HTTP CPS
1	400,000 CPS	350,000 CPS
2	400,000 CPS	350,000 CPS
3	450,000 CPS	400,000 CPS
Average		366,666 CPS

It was tested three times in total, and in the case of TCP CPS, it was measured at an average of 399,933 CPS. Each test considered the step immediately below the CPS, starting with 100,000 CPS and increasing by 200 CPS, where TCP or HTTP message misses occur, to be the maximum CPS. In the case of TCP, the first and third tests had a TCP message drop of 400,200 CPS, with a Max TCP CPS of 400,000, and the second test had a drop of 400,000 CPS. Similarly, HTTP CPS was measured at an average of 399,866 CPS.

4) PERFORMANCE COMPARISON RESULT

Comparative analysis was made on the overall performance between the proposed 5G security system and NGFW systems tested in NSS Labs' NGFW Performance Report [28]. In this analysis, box plots were used, where the box plot created by John W. Tukey is a graph that is used to show the distribution of data sets. A box plot represents the minimum and maximum values of data, as well as providing information at a glance such as the median, the upper quartile and lower quartile. It can further represent Interquartile ranOutlier (IQR) to show data points outside the min and max values as outliers [29].

The NGFW Comparative Report of NSS Labs contains overall performance data for 10 devices of such vendors as Cisco, Check Point, etc. By comparing the proposed system with these vendor products, it is possible to determine if the proposed system with 5G session management features employed is comparatively good or bad, in terms of performance.

When it comes to UDP Latency, to begin with, the proposed system showed the lowest latency time, except products of Fortinet and Palo Alto Networks. The product of Fortinet shows latency of 7 10us and the product of Palo Alto Networks shows latency of 13 20us, meaning that their performance capabilities are higher than the proposed system showing latency of 23 to 29us. When it comes to the second parameter, UDP Throughput, the proposed system was found to be better than vendor-products except Fortinet's. The

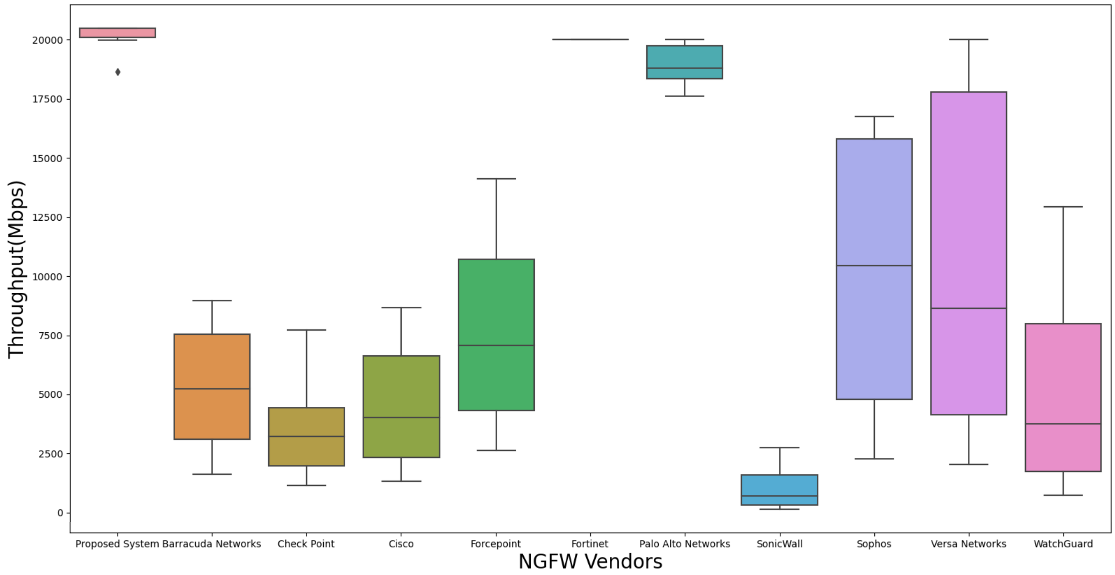


FIGURE 25. UDP throughput comparison with NGFW vendors.

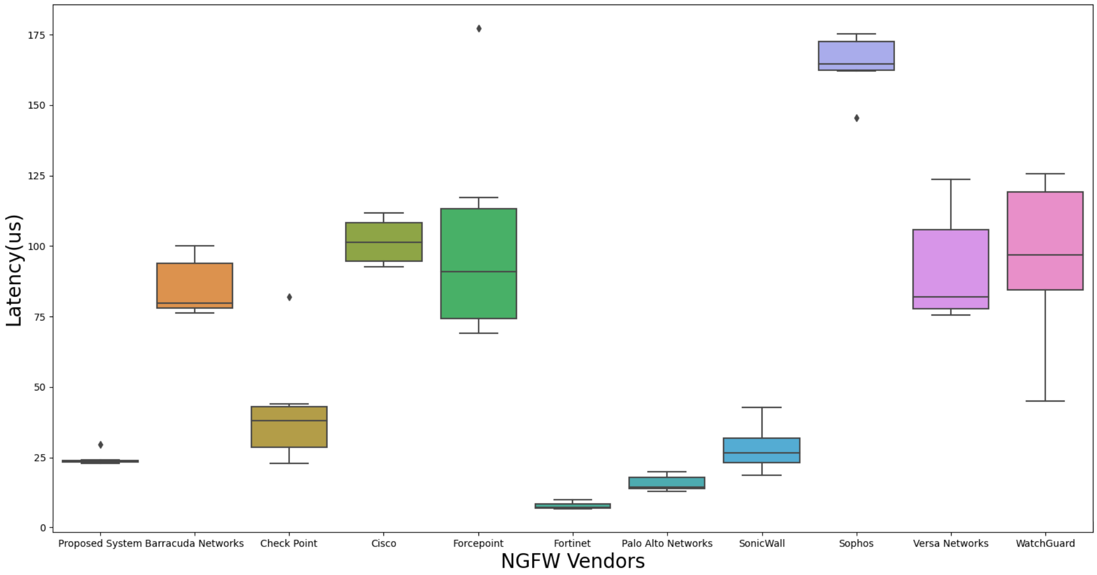


FIGURE 26. UDP latency comparison with NGFW vendors.

proposed system's UDP Throughput shows 19.62Gbps on average, whereas Fortinet device shows the best performance with 20Gbps.

When it comes to the third parameter, Max Capacity, the proposed system was found to show excellent performance compared to most of vendor-products. As for TCP protocol, whereas vendor-products show capacity of not greater than approx. 200,000 CPS, the proposed system shows capacity of nearest 400,000 CPS. As for HTTP protocol, whereas vendor-products show capacity of not greater than approx. 100,000 CPS, the proposed system shows capacity of over 350,000 CPS.

Finally, when we performed performance tests, the resource overheads of the proposed system were very reasonable. Memory showed an average usage rate of 37.8%, and CPU usage rate was between 42% and 44%.

VII. DISCUSSION

Thanks to the advancement in 5G wireless technology, 5G offers network speeds and bandwidth not less than what we could get in wire-line network. In particular, 5G networks are being used for services that require immediate response while providing microsecond latency. Recently, as the 5G is applied to medical fields, a privacy-preservation technique

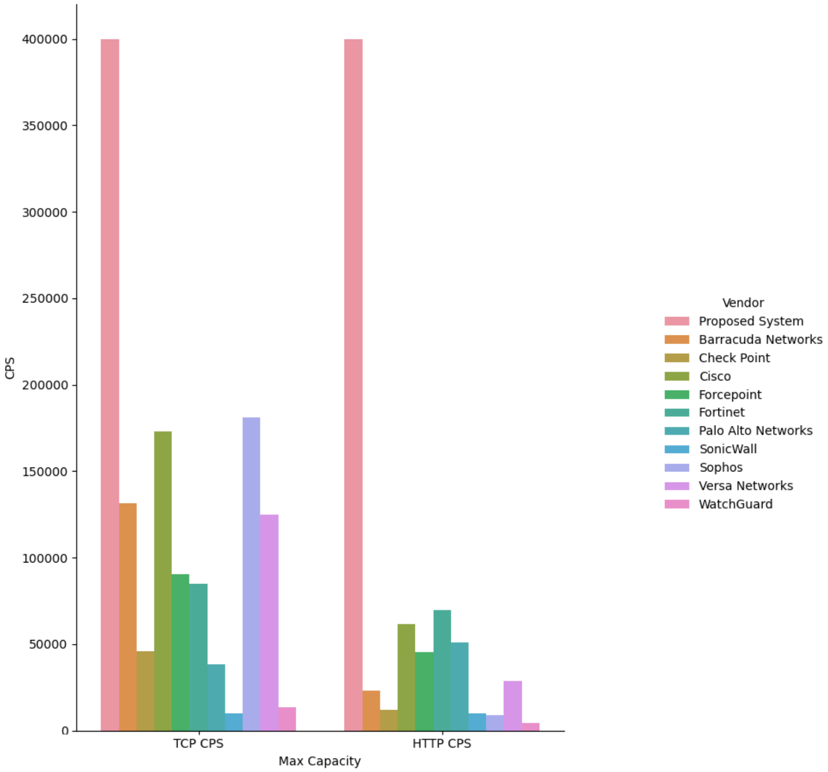


FIGURE 27. Max capacity comparison with NGFW vendors.

is also being studied to provide emergency medical systems (EMS) using 5G-based Cognitive Inspired Internet of Medical Things (CI-IoMT) [30].

5G security systems shall be engineered to achieve high-speed bandwidth comparable with, or even exceeding, those of site systems in order to provide seamless services. The scheme this paper proposes for the session management enables to identify by whom malformed packets have been transmitted, when a cyber attack is detected. In addition to that, it is found that the scheme contributes to increasing the performance via the efficient session management. Despite the foregoing, the scheme when deployed causes lagging in latency time to happen than does the existing NGFW, which is likely to give rise to a problem when providing a 5G URLLC service that is sensitive to latency time. This side effect is left behind calling for further research to rectify the drawback.

Meanwhile, the complexity in available session management techniques for the user identification leads to the architecture requiring us to reference a variety of interfaces. The complicated architecture as such possibly renders the failure in creating the user session as intended, due to various variables in real-world network environments such as wireless signal cutting-out, delay and packet drop. Therefore, complex techniques for creating sessions must be simplified such that the session management can be achieved only with critically vital interfaces. The proposed technique in this paper can perform delay time of 23 29us, UDP throughput of 19.62Gbps, and Max Capacity of 350,000 400,000 CPS. It also was verified that attackers can be identified by detecting 5G security vulnerabilities. This result can be evaluated as a study that goes beyond the session management technique studied so far or the existing security system.

VIII. CONCLUSION AND FUTURE WORK

Through our work, we validate session management techniques that require security systems available on 5G networks and present performance comparison results with other existing products. In addition, we compared and analyzed the performance with other existing products based on the NSS performance evaluation criteria. If there is a point to be supplemented, it is considered that a new control group is found and additional verification is required for the point that the data on the control group is outdated in the performance evaluation.

However, the proposed session management technique can be applied in any environment as long as it is a network configured according to 5G SA standards. In other words, it can be used in private 5G networks, which is being standardized in 5G alliances around the world. Therefore, we plan to apply and test the proposed technique for a private 5G network.

In the future, it is expected that 5G security systems provided by service providers will need to be tested and verified. In addition, study into the verification and performance of previously presented and newly proposed technologies will be required. Furthermore, the 5G service provider will create a secure 5G environment that has never existed before, as well as new and convenient services that take advantage of its benefits. However, it is also necessary to think about how to effectively design security systems for new 5G services and think about ways to build them.

REFERENCES

[1] J.-M. Park. *Electrical Components Equipment*. S.Korea First to Roll out 5G Services, Beating U.S. and China, Reuters. Accessed: Apr. 13, 2019. [Online]. Available: https://www.reuters.com/article/southkorea-5g-idUSL3N21K114

[2] *T-Mobile U.S. Taunts Rivals With SA 5G Launch*. Diana Goovaerts, GSM Association, The GSMA, Mobile World Live. Accessed: Aug. 4, 2020. [Online]. Available: https://www.mobileworldlive.com/featured-content/home-banner/t-mobile-us-taunts-rivals-with-sa-5g-launch

[3] H. Kim, J. Lee, E. Lee, and Y. Kim, ''Touching the untouchables: Dynamic security analysis of the LTE control plane,'' in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1153–1168, doi: 10.1109/SP.2019.00038.

[4] H. Kim, D. Kim, M. Kwon, H. Han, Y. Jang, D. Han, T. Kim, and Y. Kim, ''Breaking and fixing VoLTE: Exploiting hidden data channels and mis-implementations,'' in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, Oct. 2015, pp. 328–339, doi: 10.1145/2810103.2813718.

[5] S. Park, S. Kim, K. Son, and H. Kim, ''Security threats and countermeasure frame using a session control mechanism on VoLTE,'' in *Proc. 10th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Nov. 2015, pp. 532–537, doi: 10.1109/BWCCA.2015.11.

[6] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, ''Practical attacks against privacy and availability in 4G/LTE mobile communication systems,'' 2015, *arXiv:1510.07563*.

[7] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, ''LTEInspector: A systematic approach for adversarial testing of 4G LTE,'' in *Proc. NDSS*, 2018, pp. 1–15.

[8] D. Rupprecht, K. Kohls, T. Holz, and C. Popper, ''Breaking LTE on layer two,'' in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1121–1136, doi: 10.1109/SP.2019.00006.

[9] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, ''Privacy attacks to the 4G and 5G cellular paging protocols using side channel information,'' in *Proc. NDSS*, 2019, pp. 1–15, doi: 10.14722/ndss.2019.23442.

[10] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, ''New privacy threat on 3G, 4G, and upcoming 5G AKA protocols,'' in *Proc. Privacy Enhancing Technol.*, 2019, pp. 108–127, doi: 10.2478/popets-2019-0039.

[11] S. Park, H. Cho, Y. Park, B. Choi, D. Kim, and K. Yim, ''Security problems of 5G voice communication,'' in *Information Security Applications (WISA)*, I. You, Ed. Tokyo, Japan: The Institute of Electronics, Information and Communication Engineers, 2020, pp. 403–415.

[12] H. Cho, S. Park, Y. Park, B. Choi, D. Kim, and K. Yim, ''Analysis against security issues of voice over 5G,'' *IEICE Trans. Inf. Syst.*, vol. 104, no. 11, pp. 1850–1856, Nov. 2021, doi: 10.1587/transinf.2021NGP0017.

[13] G. Peinado Gomez, J. Mongay Batalla, Y. Miche, S. Holtmanns, C. X. Mavromoustakis, G. Mastorakis, and N. Haider, ''Security policies definition and enforcement utilizing policy control function framework in 5G,'' *Comput. Commun.*, vol. 172, pp. 226–237, Apr. 2021, doi: 10.1016/j.comcom.2021.03.024.

[14] *5G; System Architecture for the 5G System*, (Rel. 17), 3GPP document TS 23.501, 2021.

[15] S. Park, S. Kim, J. Oh, M. Noh, and C. Im, ''Threats and countermeasures on a 4G mobile network,'' in *Proc. 8th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Jul. 2014, pp. 538–541, doi: 10.1109/IMIS.2014.79.

[16] Y. Shi and Y. E. Sagduyu, ''Adversarial machine learning for flooding attacks on 5G radio access network slicing,'' in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6, doi: 10.1109/ICC-Workshops50388.2021.9473567.

[17] T. Fei and W. Wang, ''LTE is vulnerable: Implementing identity spoofing and denial-of-service attacks in LTE networks,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013397.

[18] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, ''Call me maybe: Eavesdropping encrypted LTE calls with ReVoLTE,'' in *29th USENIX Secur. Symp.*, 2020, pp. 73–88.

[19] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, ''LTE security disabled: Misconfiguration in commercial networks,'' in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.*, New York, NY, USA, May 2019, pp. 261–266, doi: 10.1145/3317549.3324927.

[20] *The Challenges of Fuzzing 5G Protocols*. Nccmarktedman, 5G Security & Smart Environments, NCC Group. Accessed: Oct. 11, 2021. [Online]. Available: https://research.nccgroup.com/2021/10/11/the-challenges-of-fuzzing-5g-protocols/

[21] C. Zhang, F. Ruan, L. Yin, X. Chen, L. Zhai, and F. Liu, ''A deep learning approach for network intrusion detection based on NSL-KDD dataset,'' in *Proc. IEEE 13th Int. Conf. Anti-Counterfeiting, Secur., Identificat. (ASID)*, Oct. 2019, pp. 41–45, doi: 10.1109/ICASID.2019.8925239.

[22] T. Chadza, K. G. Kyriakopoulos, and S. Lambotharan, ''Contemporary sequential network attacks prediction using hidden Markov model,'' in *Proc. 17th Int. Conf. Privacy, Secur. Trust (PST)*, Aug. 2019, pp. 1–3, doi: 10.1109/PST47121.2019.8949035.

[23] Y. Yu, J. Long, and Z. Cai, ''Session-based network intrusion detection using a deep learning architecture,'' in *Proc. Int. Conf. Modeling Decisions Artif. Intell.*, Oct. 2017, pp. 144–155, doi: 10.1007/978-3-319-67422-3_13.

[24] S. Kwon, S. Park, H. Cho, Y. Park, D. Kim, and K. Yim, ''Towards 5G-based IoT security analysis against Vo5G eavesdropping,'' *Computing*, vol. 103, no. 3, pp. 425–447, Mar. 2021, doi: 10.1007/s00607-020-00855-0.

[25] S. Park, S. Kim, K. Son, H. Kim, J. Park, and K. Yim, ''Real threats using GTP protocol and countermeasures on a 4G mobile grid computing environment,'' *Int. J. Web Grid Services (IJWGS)*, vol. 13, no. 1, p. 103, 2017, doi: 10.1504/IJWGS.2017.082060.

[26] *5G; Security Architecture and Procedures for 5G System*, (Rel. 17), 3GPP document TS 33.501, 2021.

[27] S. Park, B. Choi, Y. Park, D. Kim, E. Jeong, and K. Yim, ''Vestiges of past generation: Threats to 5G core network,'' in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)* (Advances in Intelligent Systems and Computing), vol. 1195, L. Barolli, A. Poniszewska-Maranda, and H. Park, Eds. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-50399-4_45.

[28] T. Skybakmoen, ''NSS labs 2018 NGFW comparative report performance,'' NSS Labs, Austin, TX, USA, Tech. Rep. 071718, Jul. 2018. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/nss-labs-2018-ngfw-comparative-report-performance.pdf

[29] R. McGill, J. W. Tukey, and W. A. Larsen, ''Variations of box plots,'' *Amer. Statistician*, vol. 32, no. 1, p. 12, Feb. 1978.

[30] B. D. Deebak, F. H. Memon, S. A. Khowaja, K. Dev, W. Wang, and N. M. F. Qureshi, ''In the digital age of 5G networks: Seamless privacy-preserving authentication for cognitive-inspired internet of medical things,'' *IEEE Trans. Ind. Informat.*, early access, May 3, 2022, doi: 10.1109/TII.2022.3172139.

SEONGMIN PARK received the B.S. degree in physics and electronic engineering and the M.S. degree in management of technology from Sogang University, Seoul, South Korea, in 2009 and 2015, respectively. He is currently pursuing the Ph.D. degree in information security engineering at Kookmin University, Seoul. From 2009 to 2013, he worked as a Researcher with the Core Network Development Laboratory, LGUplus Company, Seoul. Since 2013, he has been working as a General Researcher with the Korea Internet Security Center, Korea Internet & Security Agency, Naju, South Korea. His research interests include mobile security, network security, convergence security, and AI security analysis.

SUNGMOON KWON received the B.S. degree in information and computer engineering and the Ph.D. degree in computer science and engineering from Ajou University, Suwon, South Korea, in 2013 and 2020, respectively. Since 2020, he has been working as a Deputy General Researcher with the Korea Internet Security Center, Korea Internet & Security Agency, Naju, South Korea. His current research interests include 5G security, network security, and applied machine learning.

YOUNGKWON PARK received the M.S. degree in information security engineering from Dongguk University, Seoul, South Korea, in 2017. Since 2013, he has been working as a Deputy General Researcher with the Korea Internet Security Center, Korea Internet & Security Agency, Naju, South Korea. His current research interests include 5G security, network security, and applied machine learning.

DOWON KIM received the M.S. degree in information and computer engineering from Korea University, Seoul, South Korea, in 2010. He is currently pursuing the Ph.D. degree in information security engineering with Chonnam University, Gwangju, South Korea. Since 2005, he has been working as the Manager of the Korea Internet Security Center, Korea Internet & Security Agency, Naju, South Korea. His current research interests include information security, 5G security, and AI security monitoring.

ILSUN YOU (Senior Member, IEEE) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Japan, in 2012. He is currently working as a Full Professor with the Department of Financial Information Security, Kookmin University, South Korea. His research interests include internet security, authentication, access control, and formal security analysis. He is a fellow of the IET. He is the Editor-in-Chief of the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (JoWUA) and *Journal of Internet Services and Information Security* (JISIS). He is on the Editorial Board of *Information Sciences*, *Journal of Network and Computer Applications*, *International Journal of Ad Hoc and Ubiquitous Computing*, *Computing and Informatics*, and *Intelligent Automation and Soft Computing*.