Journal of Theoretical and Applied Information Technology
31st January 2024. Vol.102. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RELIABILITY FOCUSED DESIGN PMIPv6 PROTOCOL WITH SECURE HANDOVER IN 5GC NETWORKS

MADHAVA RAO MAGANTI[1*], DR K RAJASHEKAR RAO[2], DR. BALAJI VICHARAPU[3]

[1*]Research Scholar, Department of CSE, Dr. YSR ANUCET, Acharya Nagarjuna University, Assistant Professor, Sir C R Reddy College of Engineering. Email: madhavaraomaganti@gmail.com
[2]Director, Usha Rama College of Engineering, Telaprolu. Email: krr_it@yahoo.co.in
[3]Department of CSE,Dr.YSR ANUCET, Acharya Nagarjuna University. Email: v.balaji.anu@gmail.com

ABSTRACT

Fifth generation (5G) networks deliver Massive Machine Type Communication (M^2TC), better mobile broadband, and really dependable and minimal latency communications. To maximize these use cases, one must understand communication, 5G network segments, and architecture. These innovative network ideas require UE, RAN, and 5GC. Release 16 of the Third Generation Partnership Project included the Non-Access Level (NAL) and FG Application Protocol (FGAP) to improve RAN-5GC connectivity. A suggested outline supports reducing the conventional differences between EPC network components and improving flexibility inside the 5GC by ritualizing mobile network operations utilizing Reliability Focused Design PMIPv6 (REFDPMIPV6) in a cloud environment. The envisioned protocol defines protocol stacks and features pertinent to 5G networks, including resource allocation, data session formation, and authentication and identity processes. The protocol also discusses message flow related to Future Generation Node B (gNodeB) and UE registration. The suggested protocol exhibits resilience against a variety of assaults, successfully aligning with stated objectives, and has been rigorously modelled and validated using formal verification tools like BAN Logic and Scyther, as confirmed by simulation results.
Keywords: - *5GC, FG-RAN, PMIPv6, REFD, NS3.*

1. INTRODUCTION

Network automation is the obvious next step in network development, maximizing service utilization and supporting novel applications like Massive Machine Type Communication (M^2TC), improved mobile broadband, and really dependable and minimal latency transmissions (RDMLT) [1]. Incorporating 5G networks profoundly changes how networks are implemented and configured, moving from a static to a completely dynamic approach. Establishing standards and technology to enable future use cases and applications is crucial to building the framework for such dynamic networks, which must be in line with cutting-edge notions for networks beyond 5G. To predict 6G network evolution, present standards and specifications for critical protocols like Non-Access Level (NAL) and FG Application Protocol (FGAP) must be examined, as well as their compatibility with future deployments [2].

In part, NAL and FGAP connect the 5G Core (5GC), 5G FG Radio Access Network (FG-RAN), and User Equipment (UE). These protocols control User Plane (UP) configuration, network registration, and handover, among other network activities [3]. Once UE connection with the network has been enabled, these protocols play a critical role in creating UP linkages and regulating UE mobility. They have a considerable impact on Quality of Service (QoS) and network dynamics. These protocols were created by the Third Generation Partnership Project (3GPP), and they have changed over time. The initial NAL specification was published in 2008, whereas S1 Application Protocol (S1AP), which later became FGAP, was originally released in 2007 [4][5].

Heterogeneous networks, or HetNets, are radio networks that use IoT, VANET, and WLAN technologies that cover macro cells and small cells. HetNets aim to boost user capacity and network coverage [6]. Small cells can be added to the network to improve performance depending on macro cell presence, ambient circumstances (open or covered), and population density. Small cell incorporation within 5G networks affects several things [7].

Microscopic cells make it easy for devices like M^2TCs to connect to the network, relieving high-capacity macro cells. Small cells promote Really Dependable and Minimal Latency Transmissions by improving UE signal reception and latency. Increased small cell power further improves network efficiency and significantly lowers UE latency, especially for high data rate

applications like high-definition live video streaming. Inconvenient interference between User Equipment (UE) and Base Stations (BS) results from the coexistence of numerous cells supported by varied technologies. Within the coverage area of each cell, various resources are distributed in order to reduce this interference. The use of directional antennas and allocating distinct frequencies to each cell are examples of strategies. The cellular network can successfully handle the enormous data traffic needs posed by mobile users while users, depending on their speeds, fluidly migrate between multiple cells. This is accomplished by sparingly reusing frequencies and regulating coverage and aggregation of Base Stations (BSs).

In 5G networks, a User Equipment (UE) can be connected in one of three ways, with the gNodeB (gNB) displaying the radio resource control (RRC) status as RRC-Idle, RRC-Connected, or RRC-Inactive. Mobility management must choose the principal Base Station (BS) for service while the UE is in RRC-Idle because it is switched on but not registered with any Base Station (BS). In RRC-Connected or RRC-Inactive modes, UEs receive radio channels and register [8, 9]. To improve service quality, mobility management must dynamically change the UE's BS based on location and signal strength [10, 11].

Validation requires ongoing evaluation of method definitions and implementation. Inherently handling different characteristics, protocol standards define messages for system components depending on unique situations and states. NAL and FGAP protocols tutorials are valuable for academics and businesses in addition to 3GPP standards. It tests 5G enthusiasts and others' protocol knowledge. The gNodeB (i) Network Service Provider (NSP) architecture considers a new macrocell.

After connecting this macrocell to the 5G Core datacenter, the 5G FG-RAN architecture begins. One for the Control Plane (CP) and one for the User Plane (UP), both abstracted, gNodeB creates two primary 5GC links. A wireless channel for further UE connections is opened when gNodeB joins the network and registers. The NAL and FGAP protocols now work together. After connecting wirelessly to the gNodeB, UE (ii) transmits the 5GC the initial registration message. GNodeB intermediates all UE control messages. When a UE starts UP communication, the 5GC connects to gNodeB to open a channel. Once UP is established, the UE can interchange data with the Data Network (DN) and deregister. The device is turned off and gNodeB deregistered [12].

2. INTERFACES AND COMPONENTS OF 5G SYSTEMS

Several research articles on security measures have improved the Reliability Focused DesignPMIPv6 (REFDPMIPV6PMIPv6) protocol's dependability. 5GS aims to connect user devices (UEs). The 5GS creates User Plane (UP) pathways to Data Networks (DNs) and allows UEs to register for accounts via Control Plane (CP) operations. These CP activities require components to be moved from the network's edge to the core. 3GPP [13] created a reference point-based design to facilitate 5GS component communication.

Accordingly, we constructed a 5GS design that follows the 3GPP reference architecture and explains the NAL and FGAP protocols (Fig. 1). A key part of the 5GS architecture is the 5G Core (5GC) and FG-RAN. Uu connects UE and FG-RAN instead of FG and 5GC. So, all UE connections to the 5GC are through FG. A basic description of the 5GC architecture follows to explain general operations and NAL and FGAP procedures.

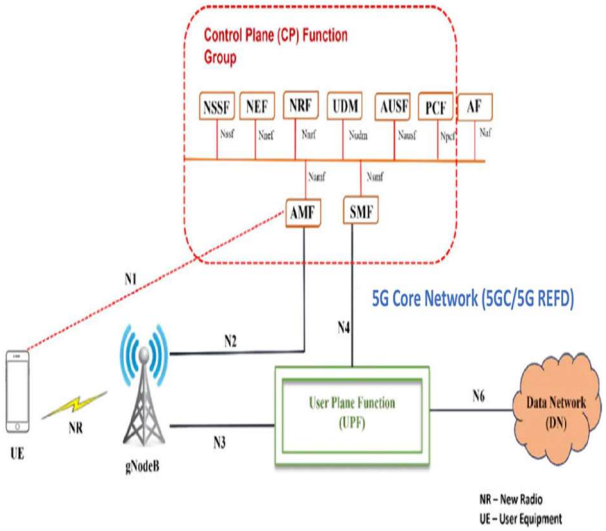

Fig. 1. Reliability Focused Design For The 5G Core (5GC).

1. A. 5G Core (5GC)

The Reliability Focused Design (REFDPMIPV6) architecture was introduced with the 5G Core (5GC) in Release 15, a major milestone [14]. Like cloud environments, this architectural paradigm emphasizes code decoupling by separating code into microservices. Fig. 1 shows that the 5GC has Ten Network Functions (NFs), each of which provides a variety of services, such as selecting Network Slices (NSs) for the Network Slice Selection Function (NSSF) and analytical tools for the Network Data Analysis Function. The User

Plane Function (UPF), Access and Mobility Function (AMF), and Session Management Function (SMF) are the priority 5GC NFs for NAL and FGAP protocols. These NFs are strongly related to NAL and FGAP procedures, hence this course emphasizes them. More detailed is Cardoso et al.'s [15] 5GC function analysis. The AMF manages any signals that isn't linked to user data, such as mobility and security, in addition to CP communication. SMF controls user data flow and session formation [14]. UE transfers NAL user data requests to FG-RAN via wireless. Before being transported from the FG-RAN to the 5GC AMF, NAL packets are FGAP-encompassed. AMF activities provide indirect interaction between FG-RAN and SMF for necessary communications. Packet Forwarding Control Protocol (PFCP) links SMF and UPF via the N4 reference point, enabling user data traffic processes.

The GPRS Tunnelling Protocol (GTP)-U is used to link directly to FG-RAN or create a GTP tunnel for UP traffic, symbolizing user data management [16]. FG-RAN connection requests trigger UPF to construct a GTP tunnel for each UE, filtering network traffic and gathering data for processing. NAL and FGAP use N1 and N2 reference points for CP communication. The NAL protocol uses the N1 reference point between the UE and AMF, while the FG-RAN needs the N2 reference point. The N11 reference point also allows AMF and SMF to send NAL messages for a specific SMF instance. AMF uses N11 to send NAL messages. We will explain FG-RAN's NAL and FGAP protocols to help you understand its major components and interactions.

2. B. Radio Access Network Of The Future Generation (FG-RAN)

The 5G Core (5GC) and gNodeB (FG-RAN component) communicate across the Future Generation (FG) logical interface (FGAP). This interface allows the separation of CP and UP (FG-C and FG-U). As illustrated in Fig. 2, these interfaces are further classified into TNL and RNL groups. This framework defines FG-U as UP over the FG interface and FG-C as CP. The FG-RAN node and 5GC must communicate using TNL network packets. The Radio Network Layer emphasizes mobile network access control. FG-C TNL stack over IP uses SCTP as its transport layer. SCTP offers a reliable signaling channel for the FG-RAN node and AMF.

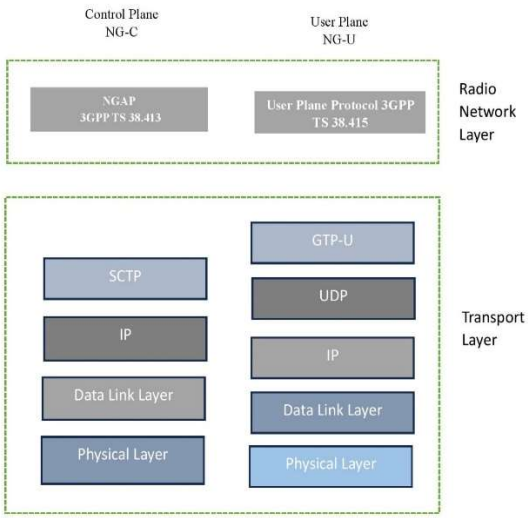

Fig. 2. FG-C and FG-U protocol stack.

The FG User plane Interface (FG-U) stack is enabled via UDP via a GTP-U tunnel. UDP can send non-guaranteed User Plane (UP) communication between the FG-RAN node and the UPF. After a quick introduction of the 5G System's pieces and interfaces, the next sections will describe NAL and FGAP.

3. NON-ACCESS LEVEL (NAL):

The N1 reference point controls NAL protocol communication between user equipment (UE) and the Access and Mobility Function (AMF). NAL also communicates N11 reference points over HTTP between AMF and Session Management Function. UEs can access the network over Wi-Fi or DOCSIS, or via 3GPP networks utilizing gNodeB. Only 3GPP networks are considered in this analysis. 3GPP highlights NAL protocols for UE mobility, authentication, identification, general UE configuration updates, and security control mode activities. NAL also supports Procedures for Session Management, which create and maintain data contact between the UE and the Data Network.

In addition to transporting these services, NAL supports SMS, LPP, LCS, UE Policy Containers, SOR Transparent Containers, and UE Parameters [17].Five GS Mobility Management (5GMM) and Session Management (5GSM) message groups serve these three NAL functions. 5GMM allows registered, mobile, and secure communication between the UE and AMF via 5GSM [16]. When UE interacts with SMF through AMF, 5GSM controls UE-DN connection. Communication channels like the Uu interface and N3 reference point help the overlay network manage connections, known as

PDU sessions. It supports IPv4, IPv6, Ethernet, and unorganized PDU sessions.

3. A. Procedures

Following is a list of the six basic operations that the 5GMM messages support:

1. **Registration-** This procedure regulates registration status, facilitates information flow between the UE and 5GC, and informs the AMF of the intended registration type.
2. **Primary Authentication and Key Agreement-** Validates and authenticates communication between the UE and 5GC. Two important authentication protocols are EAP and 5G Authentication and Key Agreement.
3. UE **Identification**- This job provides specific UE identification within the 5GC. The 5GC may request the Extended Unique Identifier (EUI)-64, Subscription Concealed Identifier (SUCI), International Mobile Equipment Identifier (IMEI), and Software Version Number (IMEISV). PEI represents the final two identifications.
4. **Transport**- Handles SMS, NAL communications, UE policy container data, and other messages. It moves payloads from AMF to UE.
5. **Security Mode**- The key generated via the primary authentication and key agreement is used to build the NAL security context between the UE and AMF. This context is reinforced by ciphering and integrity algorithms.
6. **Generic UE configuration update-** Manages mobility and access changes.

Only one process is supported by the 5GSM messages:

PDU sessions are created, modified, and terminated by session management. The authentication and authorization methods are included. Resource management covers network slicing, Data Networks (DNs), and QoS.

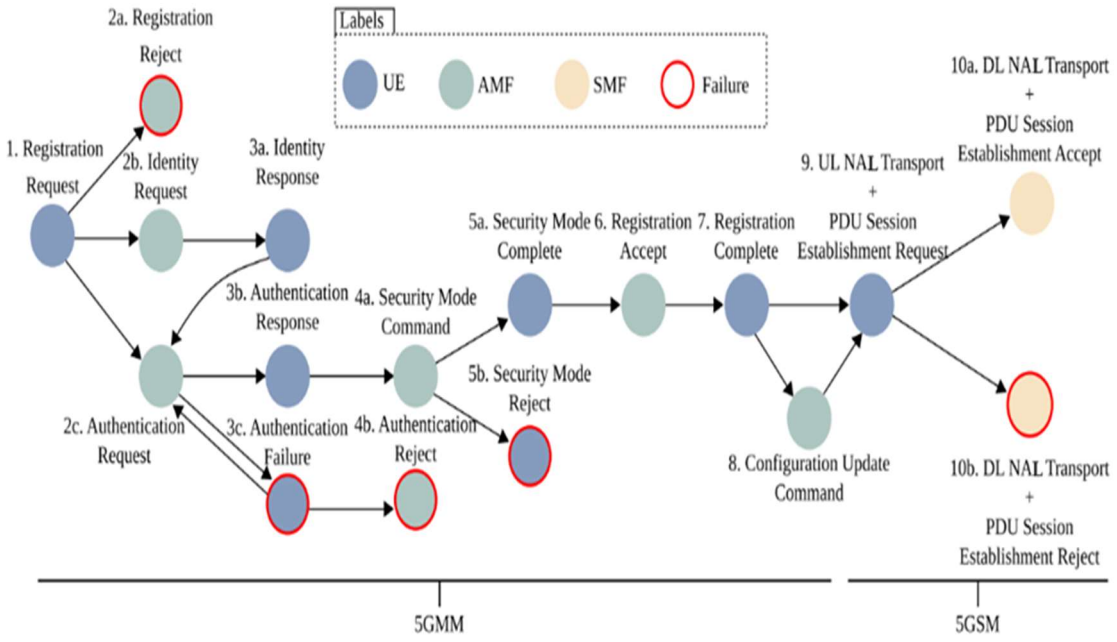

Fig. 3. Message Flow In The Non-Access Level (NAL)

3. B. Message flow

We provide the NAL message flow for UE registration in this study to analyze the protocol (Fig. 3). Messages (1)–(8) relate to 5GMM functions. The 5GC responds to the UE's Registration Request with the initial transmission. This message includes initial, mobility, periodic, and emergency registration information. Since the first registration scenario we focus on in this tutorial lacks context, the UE must offer a 5GS mobile identity, such as SUCI, or interim identifiers, such as the 5G Globally Unique Interim Identifier (GUI^2), for identification during the first network registration. The first registration includes requests for Local Area Data Network (LADN) and Network Slices as an instance of Network Slice Selection Assistance Information (NS^2AI), which has two values: Slice/Service Type (SST) and an optional Slice Differentiator (SD). However, sending this information in clear text without protection is impossible.

Fig. 3 shows the three possible registration request responses from AMF: registration refuse (2a), identification request (2b), or authentication request (2c). Registration Reject (2a) alerts the UE to protocol errors or invalid values in the Registration Request. An Identity Request (2b) is triggered if the UE transmits an unidentified identity in a registration request, such as a 5G-GUI[2] the AMF is unaware of. 5GC sends an Identity Request and Identity Response (3a) to the UE for a specific identification. After identification, the user sends an authentication request (2c), starting primary authentication and key agreement.

Authentication answer (3b) delivers the authentication challenge answer to the 5GC, which examines the value and completes primary authentication if the key matches. The UE can broadcast an Authentication Failure (3c) message to synchronize the Sequence Number (SQN) and offer a fresh challenge in the event of an authentication failure. In this flow, 5GC sends an Authentication Reject (4b) message to cease primary authentication. Many keys generate MAC and SQN validation failures when they fall outside the allowed range, causing most primary authentication issues.

After exchanging key agreement, primary authentication, and identity messages, the UE and AMF secure NAL communications. The Security Mode Command (4a) packet labels AMF's NAL security algorithms for ciphering and integrity checks. UEs that support the selected NAL algorithm receive the Security Mode Complete (5a) message. UEs send Security Mode Reject (5b) messages if they cannot handle the desired security level. Security Mode Complete gives the UE a 5G NAL security environment, enabling encrypted 5GC connections.

Retransmission of NAL communications may be required due to earlier events, such as Registration Requests containing sensitive data, before the NAL security environment was created. For AMF transmission, these messages are in Security Mode Complete. Integrity requires ciphering all NAL signaling with the new security context.

The Registration Accept (6) message informs the user that 5GC has approved their registration, and it is sent to the UE once the security NAL context and authentication have been set up. This message contains the following: the UE's tracking area list (TAL), LADN, similar public land mobile networks (PLMN), authorised networking slices, service area limitations, timers for periodic update registration, and AMF's 5G-GUI[2] temporary identifier. Lastly, the UE receives the 5G-GUI[2], and AMF is notified of this via the Registration Complete (7) message. The location, NAL connection, and security of the UE are known to the 5GC. To update the UE context with new 5G-GUI[2], TAL, service area list, LADN, approved or refused NS[2]AI, MICO, network name, and more, AMF can send the Configuration Update Command (8) message.

Through the use of the following registration messages, the 5GMM state machine in the User Equipment (UE) and Access and Mobility Management Function (AMF) is updated: Request (1), Reject (2a), Accept (6), and Complete (7). State changes during the message flow are illustrated using a summarised NAL 5GMM state machine. The state changes from Deregistered to Registered Initiated (a) when the UE sends the Registration Request message to the AMF. The 5GMM state machine then marks the change from Registered Initiated to Registered (b) upon receiving the UE's Registration Accept and the AMF's Registration Complete messages. The UE may suggest one or more PDU sessions inside the 5G Core (5GC) during the registration process. The state may revert from Registered Initiated to Deregistered if the UE and AMF exchange Registration Reject messages.

5GSM features in messages (9) to (10b) about starting PDU sessions are displayed in Fig. 3. The AMF receives the UL NAL Transport with PDU sessions Establishment Request (9) from the UE. This request includes the PDU session type, requested Data Network Name (DNN), requested Single-Network Slice Selection Assistance Information (S-NS2AI), and PDU session identity. These factors enabled the 5GC to select the UPF and SMF for the PDU session. PDU Session Establishment Accept (10a) message from the selected SMF to the AMF, which encapsulates it in DL NAL Transport and forwards it to the UE, is provided by the 5GC. The PDU address, QoS guidelines, and AMBR are all included in the PDU Session Establishment Accept. The UE is notified of the reason for rejection by the DL NAL Transport and PDU sessions Establishment Reject (10b) message if the SMF rejects this PDU session. PDU session messages are used to update the state machine of the UE 5GSM SMF.

Once the PDU Session Establishment Request message is sent by the UE and received by the SMF, the PDU Session changes from Inactive to Active Pending (a). The PDU session is in the PDU Session Pending state until the UE receives and sends the PDU session Establishment Accept message to the SMF (b). As soon as the Accept message is substituted with the PDU Session Establishment Reject message, the UE's PDU Session Active Pending state turns into Inactive (c). In the final

stage, known as PDU Session Active, a UE initiates resources to communicate with a DN using 5GSM-requested PDU sessions.

4. FUTURE GENERATION APPLICATION PROTOCOL (FGAP)

FGAP is the standard protocol for Control Plane (CP) communication between the FG-RAN and the 5G Core (5GC) via the FG-C interface and the N2 reference point in the reference architecture. The FGAP interface is necessary for 3GPP and non-3GPP access networks. It is crucial to the 5G ecosystem's organization-wide communication and control. FGAP supports Paging, UE Context Management, Mobility Management, PDU Session Management, NAL Transport, Warning Message Transmission, AMF Management, AMF Load Balancing, Multiple TNL Associations, Location Reporting, and UE Radio Capability Management [18]. Effective 5G network management requires these traits. Due to the importance of FGAP in 5G networks, this lesson covers 3GPP access and the main procedures and message flow.

4. A. Procedures

The following are the four main processes that the FGAP messages support:

1. Interface management: Responsible for maintaining the FG-C interface, which sends FGAP and NAL signals. Involves managing TNL connections in the FGAP stack and selecting networking slices using PLMN in AMF. Covers connecting AMF and FG-RAN.
2. NAL Message Transport: Transports FG-RAN-AMF NAL communications. It encapsulates NAL messages in FGAP before sending them to FG-C.
3. UE Context Management: FG-RAN receives security details, PDU session context, mobile device limits, permitted networking slices, AMF connection details, UE Radio Capability, and UE Security Capabilities.
4. PDU Session Management: Controls PDU session resource provision. These resources are needed to build the data plane's Radio Interface (Uu) and FG-U interfaces with FG-RAN and 5GC.
5.
6.

4. B. Message flow

To fully analyze the FGAP protocol, we will evaluate the message flow for the initial gNodeB registration and the subsequent UE registration. Fig. 4 shows gNodeB registration items 1, 2a, and 2b with UE registration items 3, 4, 5, 6a, 6b, 7, 8a, and 8b.

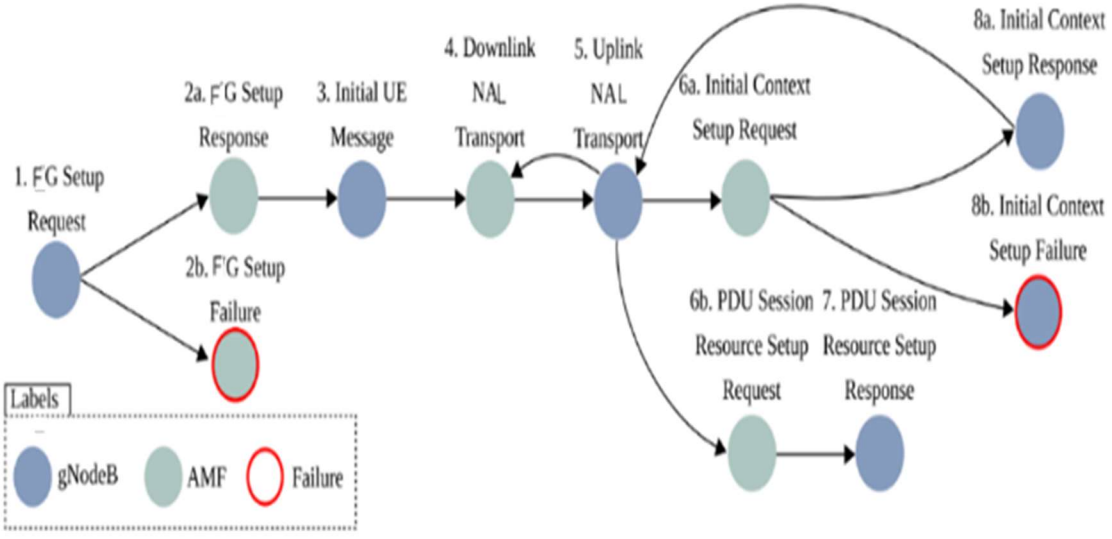

Fig. 4. FG Application Protocol (FGAP) Message Flow

The gNodeB sends the first FGAP communication, FG Setup Request, related to interface management. This message offers important gNodeB information, including the Tracking Area (TA), PLMN data, RAN node information, RAN Node Name, Global Node Identifier, and supporting Network Slice Selection Assistance Information (NS^2AI). The Paging function uses these attributes to help the TA determine which gNodeBs to broadcast. 5GC needs this information to identify 5G core-linked gNodeBs.

To completely assess the FGAP protocol, we will study the message flow for initial gNodeB registration (Fig. 4, items 1, 2a, and 2b) and subsequent UE registration (Fig. 4, items 3, 4, 5, 6a, 6b, 7, and 8a, and 8b).

The FG Setup response (2a) communication from the AMF to the gNodeB comprises the AMF name, region ID, PLMN slices, and relative AMF capacity. This data helps gNodeB choose UE AMFs based on slice support, capacity, and control load.

However, the AMF will report FG Setup Failure (2b) if the FG Setup Request is incompatible. Thus, FG-C control flow is temporarily halted until the issue is resolved. Incompatibility includes unsupported slices, unidentified TACs, and others.

FGAP communications update the FG-C state machine between FG-RAN and AMF. After receiving the FG Setup Request, the FG-C state machine advances from Inactive to Pending (a), Active (b), and perhaps Inactive (c) if the Response fails. After FG-C is formed, gNodeB can send NAL signaling to AMF using FGAP. Initial UE messages (3) signal UE NAL to AMF. The initial NAL signaling Registration Request is generally provided.

The FGAP protocol sends FG-RAN data and NAL messages after registration. Starting PDU sessions requires sending Initial Context Setup Request (6a), Initial Context Setup Response (8a), PDU Session Resource Setup Request (6b), and PDU Session Resource Setup Response (7). The data plane channel is set up based on FGAP message exchanges, allowing the UE to communicate data to the Data Network (DN) utilizing the PDU session.

To comprehend FGAP message flow state changes, a compressed PDU session source state machine is provided. This state machine demonstrates the changes from PDU Session Resource Inactive to Pending (a), Active (b), and perhaps Inactive (c) upon successful creation.

The 5G network design relies on the FGAP protocol to facilitate resource management and gNodeB-AMF communication.

5. PROPOSED REFDPMIPV6PMIPv6 Protocol

The handover authentication method we propose in this section enables secure communication between UE and NF in an application situation. Protocol registration and initial access are independent handover authentication processes. This section's notation standards are summarized in Table 1.

Table 1. Notations

Notation	Description
UE	user equipment
UF	utilization function
AAnF	AKMA anchor function
AUSF	authentication server function
UDM	unified data management
ARPF	Repository for authentication credentials and processing function
ID_A	Identifier of A
AID_{A-B}	Identifier that is anonymously used between A and B
K_A	Secret Key of A
K_{AKMA}	Utilising an Anchor Key Intermediate Between UE and AUSF/AAnF Derived From K_{AUSF}
K_{UF}	A secret key that is utilised between UE and UF is obtained from K_{AKMA}.
X, Y	ECDSA private key
Seq	Sequence Number
n_x	A nonce of x
SK	Session Key
HM	Hash-Based Code for Message Authentication

A. Registration and Initial Access

User Equipment (UE) and Authentication Server Function (AUSF) exchange the secret key KAUSF during 5G initial authentication registration. The UDM/ARPF authorizes the app. The Application Authentication Function (AAnF) receives K_{AKMA} from AUSF during initial access. K_{AUSF} buys K_{AKMA} and A-KID for UE and AUSF. UE uses Ua* to generate KUF to access UF after acquiring application approval. K_{UF}, derived from K_{AKMA}, is necessary for safe UE-AAnF communication across the Ua* reference point. Figure 5 shows the registration and initial access phase layout of the suggested protocol to demonstrate key interactions.

The suggested handover authentication technique is described in detail below:

Step 1-1: AUSF sends a Nudm_UEAuthentication_ to start the 5G initial authentication procedure. To retrieve the UE's subscriber credentials and authentication details; send a message to UDM/ARPF.

Steps 1-2: The UDM/ARPF determines whether to make KAKMA and provides the AUSF the Nudm_UEAuthentication_Get Response message with the necessary information. Using the routing identifier acquired from UDM/ARPF, AUSF deduces KAKMA and A-KID from KAUSF. Before talking to UF, UE also derives KAKMA and A-KID from KAUSF.

Steps 1-3: To choose AAnF, AUSF utilizes the AAnF Selection method. In the Naanf_AKMA_KeyRegistration Request message, AUSF informs AAnF of the SUPI and KAKMA.

Steps 1-4, The SUPI and KAKMA are stored by AAnF, and during re-authentication processes, AUSF produces new AKMA key material and transmits it to AAnF in place of keeping the previous key material.

Step 2-1: The UE creates KAKMA and A-KID from KAUSF and sends A-KID and an Application Session Establishment Request message to AF(1) before interacting with it.

B. Phase of handover using Push-Key Option

The suggested protocol divides the handover phase into the Push key and Pull key choices. Before the handover choice, both solutions follow the same process, but they differ in terms of when the UE's context is supplied. Handover occurs faster than UE movement in the first choice, Push Key. The handover decision states that the UE asks UF(1) to send the context needed for handover to UF(2). Using the context it has been given by UF(1), UF(2) authenticates and exchanges keys with the UE. Figure 6 depicts the handover phase using the push key option.

Step 3-1: When the handover scenario is detected by the UE, the UE constructs the anonymous identifier $AID_{UE\text{-}UF(1)}$ using its identify and Seq1. By avoiding identification of UE by parties other than the communication participants—including attackers—$AID_{UE\text{-}UF(1)}$ ensures UE's anonymity. To move the context that is stored in UF(1) to UF(2), UE sends an Application Handover Decision message to UF(1).

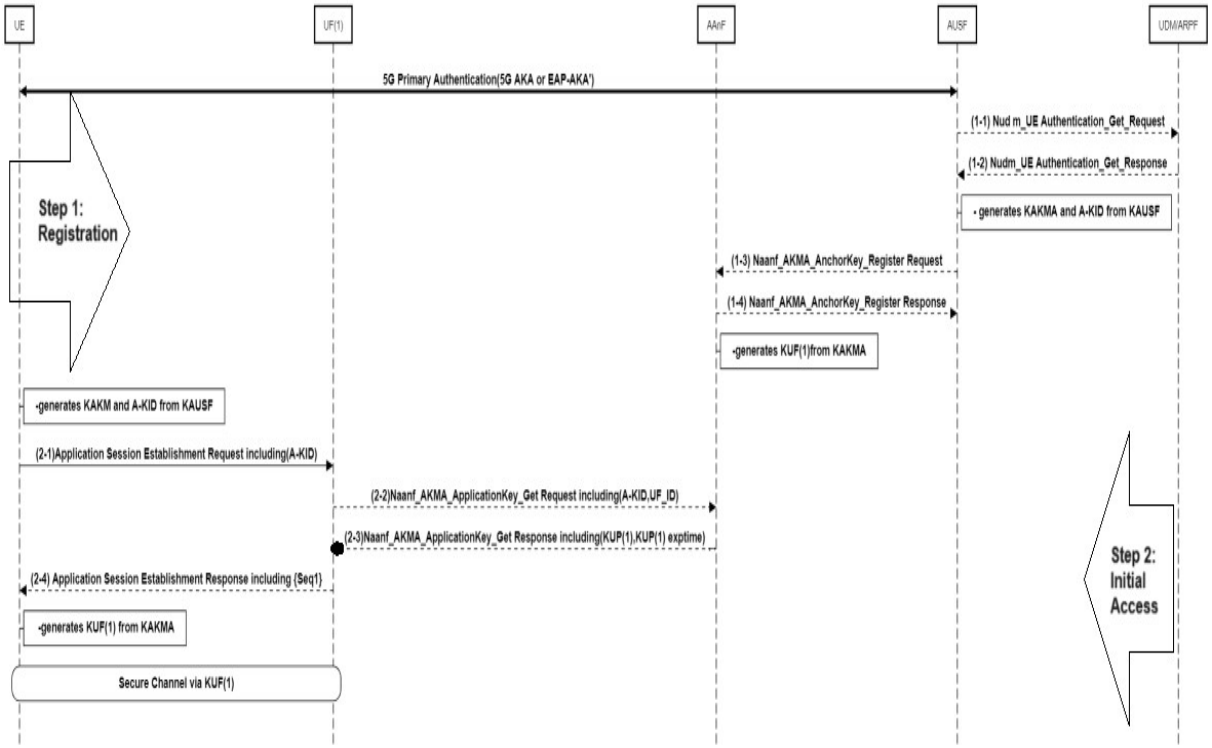

Fig. 5. Registration And Initial Access Phase

The message authentication code HM1 created by KUF(1) between UE and UF(1) at this time serves to safeguard the integrity of Application Handover Decision message.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step 3-2: After receiving the Application Handover Decision message from the UE, the UF(1) uses $AID_{UE\text{-}UF(1)}$ and Seq1 to confirm the HM1 and restore the UE's identifiers (ID_{UE}). The Application Handover Context Transfer message, which includes UE contexts like $K_{UF(1)}$, ID_{UE}, and Seq1, is then sent from UF(1) to UF(2) over a secure channel.

Step 3-3: UF(2) saves the contexts of UE ($K_{UF(1)}$, ID_{UE}, and Seq1) and sends UF(1) an Application Handover Context Transfer Complete message in response to UF(1) delivering an Application Handover Context Transfer message.

Steps 3–4: UE moves to UF(2), attaches, and then sends an Application Handover Request message to UF(2). The Application Handover Request message contains the following: the anonymous identifier ($AID_{UE\text{-}UF(1)}$), the recipient's identification ($ID_{UF(2)}$), a randomly generated nonce (n1), the ECDSA public key (XG), and the message authentication code (HM2). Furthermore, the integrity of the Application Handover Request message is safeguarded by HM2, which is generated by $K_{UF(1)}$.

Step 3-5: UF(2) first confirms HM2 with KUF(1) and then tests $AID_{UE\text{-}UF(1)}$with Seq1. We assume that $AID_{UE\text{-}UF(1)}$and HM2 are reliable. Then, UF(2) computes a new anonymous identifier ($AID_{UE\text{-}UF(2)}$), an ECDSA public key (YG), an ECDSA private key (Y), a sequence number (Seq2), and a randomly generated nonce (n2). UE's ECDSA public key and UF(2)'s newly created ECDSA private key (Y) are used to compute the session key (SK). Then, UF(2) transmits the Application Handover Response message with the following information: AIDUE, UF(2), IDUF(2), n1, n2, and YG. Through the generation of hash-based message authentication codes (HM3 and HM4) using the session keys SK and KUF(1), respectively, the integrity of the Application Handover Response message is safeguarded.

Step 3-6: The UE checks HM4 and $AID_{UE\text{-}UF(2)}$ through KUF(1) and IDUE after receiving the Application Handover Response message. UE can trust the Application Handover Response message and save the succeeding sequence number Seq2 if HM4 and IDUE are both valid. Then, using its ECDSA private key (X), UF(2)'s ECDSA public key (YG), and nonce's produced by both participants, UE determines the session key (SK). UE confirms HM3 using session key SK and learns that UF(2) accepts SK for current session. UE transmits Application Handover Key Confirm message to UF(2) along with n2 and HM5 that are secured by SK.

Steps 3–7: To ensure that the session key is safely shared with the UE, UF(2) checks the HM5 contained in the Application Key Confirm message. If HM5 is legitimate, UF(2) informs AAnF that UE and UF(2) handover authentication was successful.

Journal of Theoretical and Applied Information Technology
31st January 2024. Vol.102. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

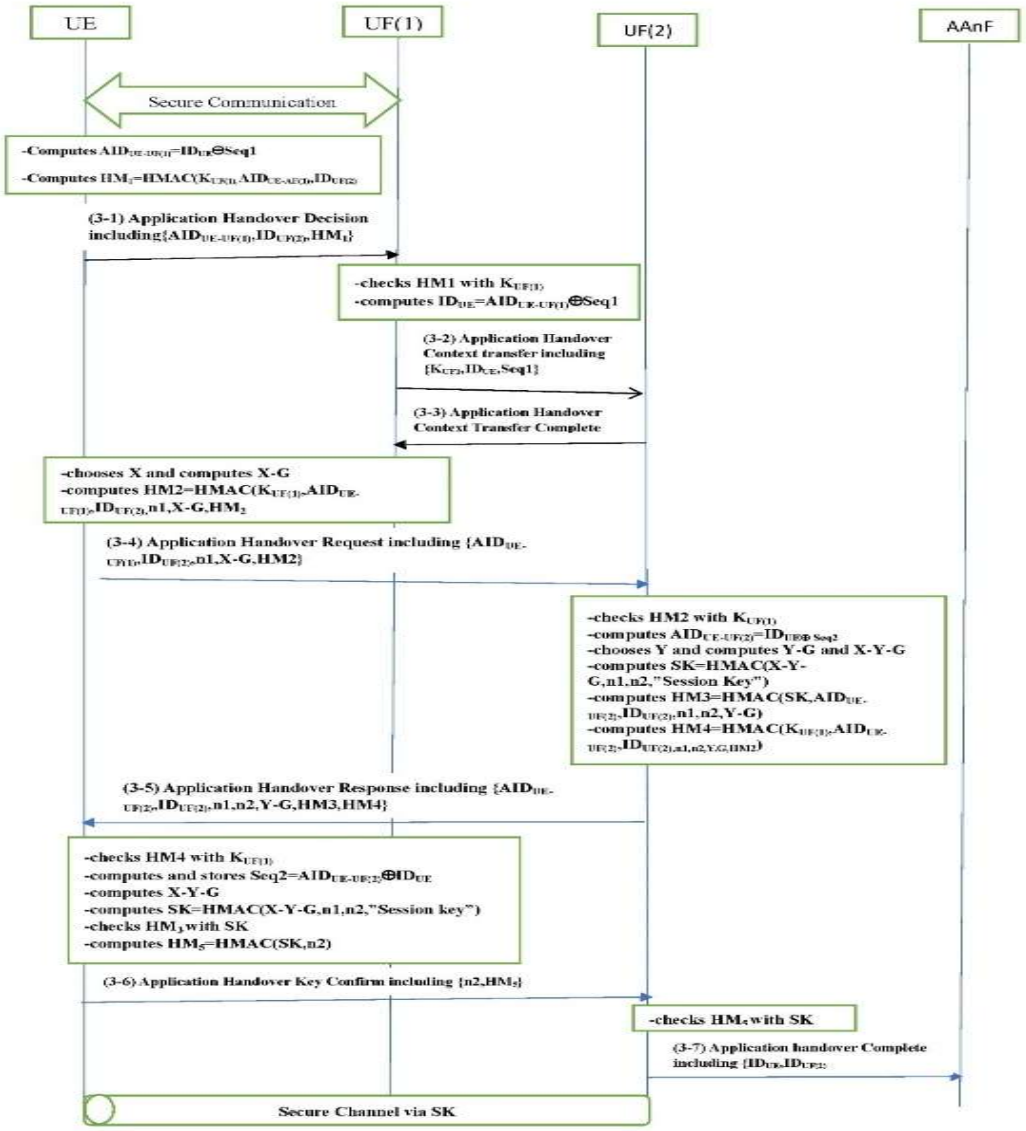

Fig 6. Handover Phase With Push Key Option

5.C. Handover Phase with Pull Key option

In contrast to the push key option mentioned above, the pull key option prompts UF(2) to ask UF(1) for the context of the UE during the handover phase. Using the context that UE has been given from UF(1), UF(2) initiates authentication and key exchange with UE. Figure 7 depicts the handover step using the pull key option.

Step 3-1: UE produces an anonymous identifier $AID_{UE\text{-}UF(1)}$, an ECDSA public key (X) and private key (XG), as well as a nonce (n1) that was chosen at random. Application Handover Request messages are sent to UF(2) by UE when it switches to the new network, which includes UF(2). Application Handover Request message contains the message authentication code (HM1) secured by KUF(1), $AID_{UE\text{-}UF(1)}$, n1, XG, and the identification of the prior application function (IDUF(1)).

Step 3-2: The UF(2) transmits the Application Handover Context UE sends UF(1) a request message.

Step 3-3: UF(1) verifies HM1 with KUF(1) after receiving the Application Handover Context Request message from UF(2). UF(1) then extracts IDUE from $AID_{UE-UF(1)}$. UF(1) can now send KUF(1) and IDUE to UF(2) through a secure channel and verify that the previously accessible UE has requested handover.

Steps 3–4: After receiving KUF(1) and IDUE from UF(1), UF(2) generates the sequence number Seq2, the ECDSA private key Y, the ECDSA public key YG, and a randomly generated nonce n2. UE's ECDSA public key (XG) obtained in step 3-1 above, its own private key (Y), and nonces (n1, n2) generated by both participants are used by UF(2) to calculate a new anonymous identifier $AID_{UE-UF(2)}$ and the session key (SK). The Application Handover Response message, which includes $AID_{UE-UF(2)}$, IDUF(2), n1, n2, and YG, is then transmitted by UF(2). Application Handover Response message authentication codes (HM2, HM3) are used to safeguard the communication.

steps 3-5: The UE, through KUF(1) and $AID_{UE-UF(2)}$, respectively, verifies HM3 and $AID_{UE-UF(2)}$ first. For the next handover scenario, UE now stores Seq2. X, n1, Y, G, and n2 are stored, and the session key SK is created from these. Since derived SK has been successfully shared with UF(2), UE may verify HM2 and be confident in the exchange. In addition to the n2 and HM4 that are secured by SK, the UE transmits the Application Handover Key Confirm message to UF(2).

Step 3-6: UF(2) validates the Application Key Confirm HM4 to confirm the session key is shared safely with the UE. UF(2) informs AAnF that UE and UF(2) handover authentication worked if HM5 is valid.

7. Formal Security Analysis

BAN logic [9] and Scyther [10] are used to analyze the proposed handover authentication protocol's security. Different security methods are often assessed using these tools. Key derivation based on the key hierarchy, identifier exchange, and initial authentication will be investigated during 5G registration and initial access. This is to ensure the push and pull selections' security during handover. Safeguarding the protocol against security threats is the purpose.

6. A. BAN LOGIC

BAN Logic security analysis involves idealization, assumption, aim, and derivation. Idealisation models encryption, digital signature, and message authentication code data using BAN Logic's notations and rules [9]. Assumption sets network settings and secure communication channels for the desired security protocol. Goal objectives match target security protocol standards. Final security analysis results from Idealisation, Assumption, and Goal in Derivation.

Journal of Theoretical and Applied Information Technology
31st January 2024. Vol.102. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

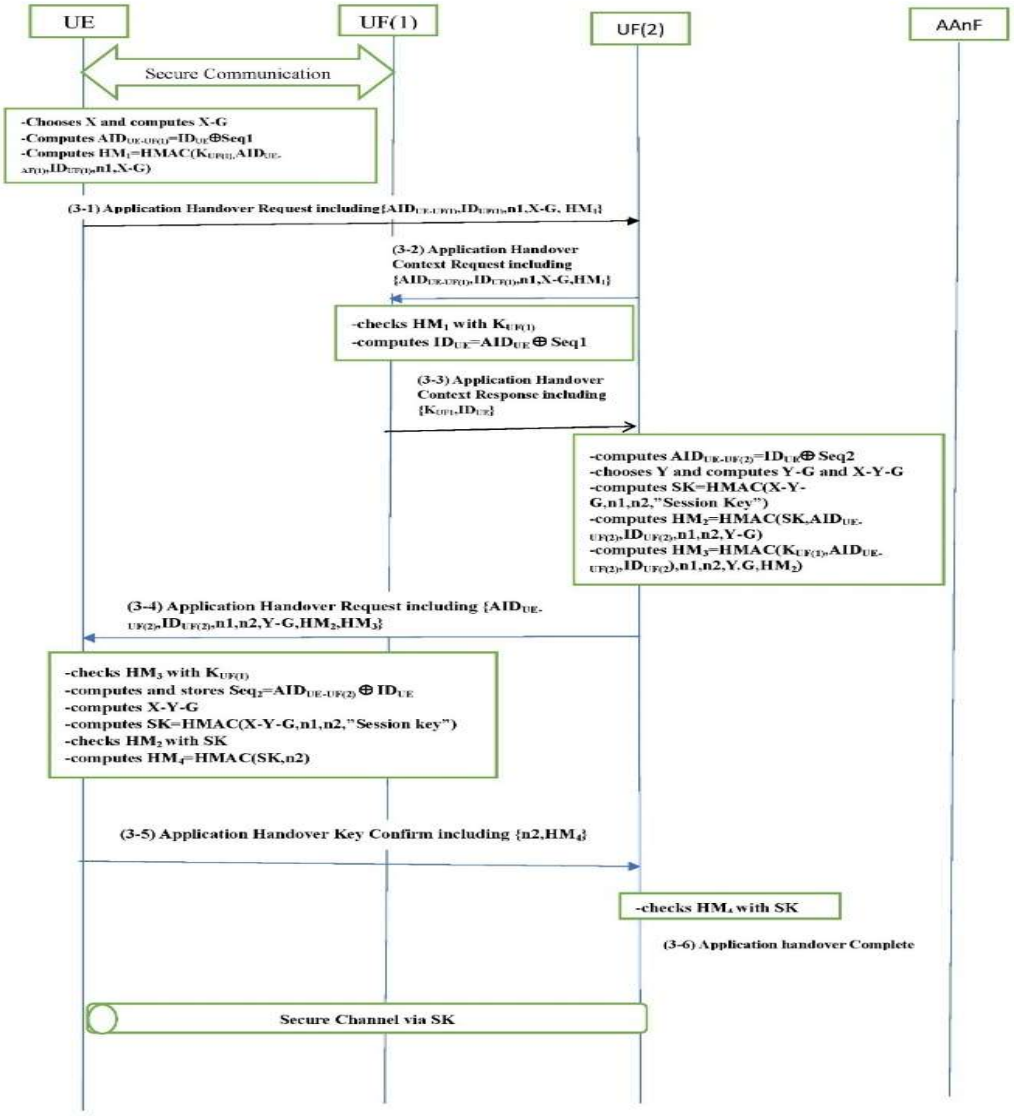

Fig. 7. Handover phase with pull key option

6.A.1. Push Key Option

- Idealization

The following equations (I1) through (I5) represent the push key option in its idealised forms. Idealisation excludes the exposed plaintext in between message transmissions.

(I1) UE→UF(1):
<AID$_{UE\text{-}UF(1)}$, ID$_{UF(2)}$, UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(1)>K$_{UF(1)}$

(I2) UF(1)→UF(2):
<UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(2), ID$_{UE}$,Seq$_1$>$_K$

(I3) UE→UF(2):
<AID$_{UE\text{-}UF(1)}$, ID$_{UF(2),n1,X.G}$,UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(2)>K$_{UF(1)}$

(I4) UF(2)→UE:
<AID$_{UE\text{-}UF(2)}$, ID$_{UF(2),n1,n2,Y.G}$,UE$\overset{SK}{\Leftrightarrow}$UF(2),UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(2)>K$_{UF(1)}$

(I5) UE→UF(2)
<n2, UE$\overset{SK}{\Leftrightarrow}$UF(2)>$_{SK}$

- Assumption

(A1) UF(1)|≡ UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(1)
(A2) UF(1)|≡ #($AID_{UE-UF(1)}$)
(A3) UF(2) |≡ UF(1) $\overset{K}{\Leftrightarrow}$ UF(2)
(A4) UF(2) |≡ #(Seq_1)
(A5) UF(2) |≡ UF(1) |⇒ UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(2)
(A6) UF(2) |≡ #(Seq_1)
(A7) UF(2) |≡ $\overset{Y.G}{\Rightarrow}$UF(2)
(A8) UF(2) |≡ #(n_2)
(A9) UE |≡ UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(2)
(A10) UE |≡ #(n1)
(A11) UE |≡ $\overset{X.G}{\Rightarrow}$UE

- Goal

(G1) UF(1) |≡ UE |≡ $AID_{UE-UF(1)}$
(G2) UF(1) |≡ UE |≡ UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(1)
(G3) UF(2) |≡ UE |≡ $AID_{UE-UF(1)}$
(G4) UF(2) |≡ UE$\overset{SK}{\Leftrightarrow}$UF(2)
(G5) UE |≡ UF(2) |≡$ID_{UF(2)}$
(G6) UE |≡ UF(2) |≡ UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(2)
(G7) UE |≡ UF(2) |≡ UE$\overset{SK}{\Leftrightarrow}$UF(2)
(G8) UE |≡ UE$\overset{SK}{\Leftrightarrow}$UF(2)
(G9) UF(2) |≡ UE |≡ UE$\overset{SK}{\Leftrightarrow}$UF(2)

- Derivation

(D1) UF(1) ⇐<$AID_{UE-UF(1)}$,$ID_{UF(2)}$, UE$\overset{KUF(1)}{\Longleftrightarrow}$UF(1)>K
(D2) UF(1) |≡ UE | ~ $\left[AID_{UE-UF(1)}, ID_{UF(2)}, UE \overset{K_{UF(1)}}{\Longleftrightarrow} UF(1)\right]$ By (D1),(A1),MM
(D3) UF(1) |≡ UE|≡ $\left[AID_{UE-UF(1)}, ID_{UF(2)}, UE \overset{K_{UF(1)}}{\Longleftrightarrow} UF(1)\right]$ By (D2),(A2),FR,NV
(D4) UF(1) |≡ UE |≡ $AID_{UE-UF(1)}$ By (D3),BC
(D5) UF(1) |≡ UE |≡ UE $\overset{K_{UF(1)}}{\Longleftrightarrow}$ UF(1) By (D3),BC
(D6) UF(2) ⇐ ⟨UE $\overset{K_{UF(1)}}{\Longleftrightarrow}$ UF(2), ID_{UE}, $Seq1\rangle_K$
(D7) UF(2) |≡ UF(1) | ~ $\left[\text{UE} \overset{K_{UF(1)}}{\Longleftrightarrow} \text{UF}(2), \text{ID}_{UE}, \text{Seq1}\right]$ By (D6),(A3),MM
(D8) UF(2) |≡ UF(1) |≡ $\left[\text{UE} \overset{K_{UF(1)}}{\Longleftrightarrow} \text{UF}(2), \text{ID}_{UE}, \text{Seq1}\right]$ By (D7),(A4),FR,NV
(D9) UF(2) |≡ UF(1) |≡ UE $\overset{K_{UF(1)}}{\Longleftrightarrow}$ UF(2) By (D8),BC
(D10) UF(2) |≡ UE $\overset{K_{UF(1)}}{\Longleftrightarrow}$ UF(2) By (D9),(A5),JR
(D11) UF(2) ⇐ $\langle AID_{UE-AF(1)}, \text{ID}_{AF(2)}, \text{Seq}_1, \text{n1}, \text{X. G}, \text{UE} \overset{K_{UF(1)}}{\Longleftrightarrow} \text{UF}(2)\rangle K_{UF(1)}$
(D12) UF(2) |≡ UE| ~ $\left[AID_{UE-UF(1)}, \text{ID}_{UF(2)}, \text{Seq}_1, \text{n1}, \text{X. G}, \text{UE} \overset{K_{UF(1)}}{\Longleftrightarrow} \text{UF}(2)\right]$ By (D11), (D10), MM
(D13) UF(2) |≡ UE |≡ $\left[AID_{UE-UF(1)}, \text{ID}_{UF(2)}, \text{Seq}_1, \text{n1}, \text{X. G}, \text{UE} \overset{K_{UF(1)}}{\Longleftrightarrow} \text{UF}(2)\right]$ By (D11), (A6),FR,NV
(D14) UF(2) |≡ UE |≡ $AID_{UE-UF(1)}$ By (D12),BC
(D15) UF(2) |≡ UE |≡ UE $\overset{K_{UF(1)}}{\Longleftrightarrow}$ UF(2) By (D12), BC
(D16) UF(2) |≡ X.Y.G By (D11), (A7), BC, DH
(D17) UF(2) |≡ UE$\overset{SK}{\Leftrightarrow}$UF(2) By (D16), (D12), (A8), BC
(D18) UE ⇐ $\langle AID_{UE-UF(2)}, \text{ID}_{UF(2)}, \text{n1}, \text{n2}, \text{Y. G}, \text{UE} \overset{SK}{\Leftrightarrow} \text{UF}(2), \text{UE} \overset{K_{UF(1)}}{\Longleftrightarrow} UF(2)\rangle K_{UF(1)}$
(D19) UE |≡ UF(2) | ~ $\left[AID_{UE-UF(2)}, \text{ID}_{UF(2)}, \text{n1}, \text{n2}, \text{Y. G}, \text{UE} \overset{SK}{\Leftrightarrow} \text{UF}(2), \text{UE} \overset{K_{UF(1)}}{\Longleftrightarrow} UF(2)\right]$ By (D18),(A9),MM
(D20) UE |≡ UF(2) |≡ $\left[AID_{UE-UF(2)}, \text{ID}_{UF(2)}, \text{n1}, \text{n2}, \text{Y. G}, \text{UE} \overset{SK}{\Leftrightarrow} \text{UF}(2), \text{UE} \overset{K_{UF(1)}}{\Longleftrightarrow} UF(2)\right]$ By (D19),(A10),FR,NV
(D21) UE |≡ UF(2) |≡$ID_{UF(2)}$ By (D20),BC
(D22) UE |≡ UF(2) |≡ UE $\overset{K_{UF(1)}}{\Longleftrightarrow}$ $UF(2)$ By (D20), BC

(D23) UE |≡ UF(2) |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$
By (D20), BC
(D24) UE |≡ X.Y.G
By (D19), (A11), BC, DH
(D25) UE |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$
By (D20), (D24), BC
(D26) UF(2) ⇐ $\langle n2, UE \overset{SK}{\Leftrightarrow} UF(2)\rangle_{SK}$
(D27) UF(2) |≡ UE | ~ $\left[n2, UE \overset{SK}{\Leftrightarrow} UF(2)\right]$
By (D26), (D17), MM
(D28) UF(2) |≡ UE |≡ $\left[n2, UE \overset{SK}{\Leftrightarrow} UF(2)\right]$
By (D27), (A8), FR, NV
(D29) UF(2) |≡ UE |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$
By (D28), BC

6. A.2 Pull Key option

- Idealization

The following equations (I6)–(I8) provide the pull key option's idealised forms.

(I6) UE→UF(2)
$\langle AID_{UE}, ID_{UF(1)}, n1, X.G, UE \overset{K}{\Leftrightarrow} UF(2)\rangle_K$
(I7) UF(2)→ UE
$\langle AID_{UE-UF(2)}, ID_{UF(2)}, n1, n2, Y.G, UE \overset{SK}{\Leftrightarrow} UF(2), UE \overset{K}{\Leftrightarrow} UF(2)\rangle_K$
(I8) UE→UF(2)
$\langle n2, UE \overset{SK}{\Leftrightarrow} UF(2)\rangle_{SK}$

- Assumption

(A12) UF(2) |≡ UE $\overset{K}{\Leftrightarrow} UF(2)$
(A13) UF(2) |≡ #(AID_{UE})
(A14) UF(2) |≡ $\overset{Y.G}{\longrightarrow}$ UF(2)
(A15) UF(2) |≡ #(n2)
(A16) UE |≡ $UE \overset{K}{\Leftrightarrow} UF(2)$
(A17) UE |≡ #(n1)
(A18) UE |≡ $\overset{X,G}{\longrightarrow}$ UE

- Goal

(G10) UF(2) |≡ UE |≡ AID_{UE}
(G11) UF(2) |≡ UE |≡ UE $\overset{K}{\Leftrightarrow} UF(2)$
(G12) UF(2) |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$
(G13) UE |≡ UF(2) |≡ $ID_{UF(2)}$
(G14) UE |≡ UF(2) |≡ UE $\overset{K}{\Leftrightarrow} UF(2)$
(G15) UE |≡ UF(2) |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$
(G16) UE |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$
(G17) UF(2) |≡ UE |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$

- Derivation

(D30) UF(2)
⇐ $\langle AID_{UE}, ID_{UF(2)}, n1, X.G, UE \overset{K}{\Leftrightarrow} UF(2)\rangle_K$
(D31) UF(2) |≡ UE |
~ $\left[AID_{UE}, ID_{UF(2)}, n1, X.G, UE \overset{K}{\Leftrightarrow} UF(2)\right]$
By (D30), (A12), MM
(D32) UF(2) |≡ UE |≡
$\left[AID_{UE}, ID_{UF(2)}, n1, X.G, UE \overset{K}{\Leftrightarrow} UF(2)\right]$ By (D31), (A13),FR,NV
(D33) UF(2) |≡ UE |≡ AID_{UE} By (D32), BC
(D34) UF(2) |≡ UE |≡ UE $\overset{K}{\Leftrightarrow} UF(2)$ By (D33), BC
(D35) UF(2) |≡ X.Y.G By (D31,(A14), BC, DH
(D36) UF(2) |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$ By (D32),(D35),(A15),BC
(D37) UE ⇐
$\langle AID_{UE-U\ (2)}, ID_{UF(2)}, n1, n2, Y.G, UE \overset{SK}{\Leftrightarrow} UF(2), UE \overset{K}{\Leftrightarrow} UF(2)\rangle_K$
(D38) UE |≡ UF(2) |
~ $\left[AID_{UE-UF(2)}, ID_{UF(2)}, n1, n2, Y.G, UE \overset{SK}{\Leftrightarrow} UF(2), UE \overset{K}{\Leftrightarrow} UF(2)\right]$ By (D37), (A16), MM

(D39) UE |≡ UF(2) |≡
$\left[AID_{UE-UF(2)}, ID_{UF(2)}, n1, n2, Y.G, UE \overset{SK}{\Leftrightarrow} UF(2), UE \overset{K}{\Leftrightarrow} UF(2)\right]$ By (D38), (A17), FR,NV
(D40) UE |≡ UF(2) |≡ $ID_{UF(2)}$
By (D39), BC
(D41) UE |≡ UF(2) |≡ UE $\overset{K}{\Leftrightarrow}$ UF(2)
By (D39),BC
(D42) UE |≡ UF(2) |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$
By (D39),BC
(D43) UE |≡ X.Y.G
By (D38),(A18),BC,DH
(D44) UE |≡ UE $\overset{SK}{\Leftrightarrow} UF(2)$
By (D39),(D43),BC
(D45) UF(2) ⇐ $\langle n2, UE \overset{SK}{\Leftrightarrow} UF(2)\rangle_{SK}$
(D46) UF(2) |≡ UE | ~ $\left[n2, UE \overset{SK}{\Leftrightarrow} UF(2)\right]$ By (D45),(D36),MM
(D47) UF(2) |≡ UE |≡ $\left[n2, UE \overset{SK}{\Leftrightarrow} UF(2)\right]$ By (D46),(A15),FR,NV

(D48) UF(2)) |≡ UE |≡ UE
$\overset{SK}{\Leftrightarrow} UF(2)$ By (D47),BC

6. B. Scyther

BAN Logic helps express and analyze modal logic authentication techniques. However, several studies have found weaknesses in BAN Logic security analysis, including inappropriate message representation in Idealisation and a lack of hash function inference rules [22–23]. Thus, BAN Logic and Scyther verify the suggested protocol. Cas J. F. Cremers suggested automated formal verification tool Scyther. Modeling, verification, and result comprise the verification process. (1) SPDL models the target security protocol. Scyther assigns roles to target security protocol communication participants and defines SPDL expressions for all protocol messages. SPDL protocol model includes global variable declaration, protocol specification, and role definition.

An additional parallel protocol can be determined by the protocol description if needed. Participants behave according to their roles. The communication message includes send and receive commands and a claim event to validate security procedures. Local variables are declared. (2) Claim events "Alive," "Niagree," "Nisynch," "Weakagree," "Running/Commit," and "Secret" confirm the SPDL protocol model. Both authentication and confidentiality are examined in each protocol model security claim. (3) Scyther provides the attack flow chart if claim events revealed security model attacks. Scyther displays 'OK' on the result screen for associated claim events if not. Figures 8 and 9 show verification results. The result screen shows "OK.", making both protocol handover alternatives secure against known threats.

The proposed approach optimizes handover over the current one. Optimized handover reduces delay when switching UFs. Compare the proposed and EAP protocols' handover delay periods to see the optimized handover. Handover delay is the signalling message's execution time until communication participants are authenticated. Handover latency for suggested protocols:

$L_{Push}=L_{Pull}$
$=3*T_{UE\text{-}UF(2)}+2 * T_{UF(1)\text{-}UF(2)}+T_{UF(2)\text{-}AAnF}+\delta$
(1)

Claim				Status	Comments
Push	UE	Push,UE2	Alive	Ok	No attacks within bounds.
		Push,UE3	Nisynch	Ok	No attacks within bounds.
		Push,UE4	Niagree	Ok	No attacks within bounds.
		Push,UE5	Weakagree	Ok	No attacks within bounds.
		Push,UE6	Commit UF2,g(x),YG,n1,n2	Ok	No attacks within bounds.
		Push,UE7	SKR k(UE,UF1)	Ok	No attacks within bounds.
		Push,UE8	SKR hm(h(YG,x),n1,n2)	Ok	No attacks within bounds.
	UF2	Push,UF22	Alive	Ok	No attacks within bounds.
		PushUF23	Nisynch	Ok	No attacks within bounds.
		PushUF24	Niagree	Ok	No attacks within bounds.
		PushUF25	Weakagree	Ok	No attacks within bounds.
		PushUF26	Commit UE,XG,g(y),n1,n2	Ok	No attacks within bounds.
		PushUF27	SKR k(UE,UF1)	Ok	No attacks within bounds.
		PushUF28	SKR hm(h(XG,y),n1,n2)	Ok	No attacks within bounds.

Fig. 8. Scyther result(push key option)

Claim				Status	Comments
Pull	UE	Pull,UE2	Alive	Ok	No attacks within bounds.
		Pull,UE3	Nisynch	Ok	No attacks within bounds.
		Pull,UE4	Niagree	Ok	No attacks within bounds.
		Pull,UE5	Weakagree	Ok	No attacks within bounds.
		Pull,UE6	Commit UF2,g(x),YG,n1,n2	Ok	No attacks within bounds.
		Pull,UE7	SKR k(UE,UF1)	Ok	No attacks within bounds.
		Pull,UE8	SKR hm(h(YG,x),n1,n2)	Ok	No attacks within bounds.
	UF2	Pull,UF22	Alive	Ok	No attacks within bounds.
		Pull,UF23	Nisynch	Ok	No attacks within bounds.
		Pull,UF24	Niagree	Ok	No attacks within bounds.
		Pull,UF25	Weakagree	Ok	No attacks within bounds.
		Pull,UF26	Commit UE,XG,g(y),n1,n2	Ok	No attacks within bounds.
		Pull,UF27	SKR k(UE,UF1)	Ok	No attacks within bounds.
		Pull,UF28	SKR hm(h(XG,y),n1,n2)	Ok	No attacks within bounds.

Fig. 9. Scyther result(pull key option)

TUF-AAnF represents the communication participants' transmission delay, and represents the processing delay for the received message. TUF-AAnF=d*, where UF and AAnF are separated by d, and is the typical transmission latency for each distance, is the formula for the transmission delay. In EAP protocols, a peer, authenticator, and authentication server correspond to the roles of UE, UF, and AAnF in the AKMA scenario, respectively, to allow for easy comparison. As a result, the EAP protocols' handover delay is as follows:

$$L_{EAP\text{-}AKA}=L_{EAP\text{-}AKA'} =4*T_{UE\text{-}UF(2)}+2*T_{UF(1)\text{-}AAbF}+3*T_{UF(2)\text{-}AAbF}+\delta \quad (2)$$

$$=L_{EAP\text{-}TLS} =8*T_{UE\text{-}UF(2)}+2*T_{UF(1)\text{-}AAbF}+9*T_{UF(2)\text{-}AAbF}+\delta \quad (3)$$

$$=L_{EAP\text{-}IKEv2} =6*T_{UE\text{-}UF(2)}+2*T_{UF(1)\text{-}AAbF}+7*T_{UF(2)\text{-}AAbF}+\delta \quad (4)$$

Table 2 lists the numerical simulation parameters suggested in [26] and [27] for handover latency. Figure 10 compares the proposed protocol's handover time to EAP methods using Table 7 numerical simulation settings. EAP protocols perform the whole authentication process for each authentication, delaying handover compared to the proposed protocol. Because they employ the same signalling message sequence, [24] and [25] cost the same, but [26], which has the most operations, has the greatest handover latency.

Table 2 Numerical simulation parameters

Parameters	Values
$T_{UE-\ UF(2)}$	1 ms
d	20 – 100 km
ς	0.05 ms/km
δ	9.5 ms

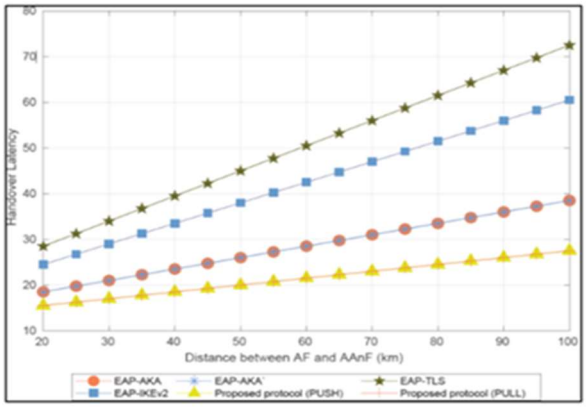

Figure 10. Handover latency vs Distance

7. CONCLUSION

5G allows clients to access multimedia services in real time, wherever they are. Users' access to NetApp's Application Functions (UFs) must be secured for secure application use. Given frequent user movement among UFs in 5G MEC situations, significant security measures are necessary. A novel security protocol that meets perfect forward secrecy, mutual authentication, safe key exchange, confidentiality, integrity, and anonymity is presented in this work. The protocol also adds push-key and pull-key optimised secure handover options to prior standards. Formal security verification of the handover scheme's two alternatives showed that REFDPMIPV6PMIPv6 meets the requirements. EAP variation study verified the protocol's computational overhead efficiency. Movement path prediction technology using artificial intelligence will be studied to improve handovers.

REFERENCES

[1] S.D.A. Shah, M.A. Gregory, S. Li, Cloud-native network slicing using software defined networking based multi-access edge computing: A survey, IEEE Access 9 (2021) 10903–10924, http://dx.doi.org/10.1109/ACCESS.2021.3050155.

[2] N.-N. Dao, et al., Survey on aerial radio access networks: Toward a comprehensive 6G access infrastructure, IEEE Commun. Surv. Tutor. 23 (2) (2021) URL https://arxiv.org/abs/2102.07087.

[3] 3GPP TS 38.413 version 16.4.0 Release 16, 5G; NG-RAN; NG application protocol (NGAP), 2021, URL https://www.etsi.org/deliver/etsi_ts/138400_138499/138413/16.04.00_60/ts_138413v160400p.pdf.

[4] 3GPP, Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS), Tech. Rep. 3GPP TS 24.301 V0.1.0, 3rd Generation Partnership Project-3GPP,2008, https://www.3gpp.org/ftp/Specs/archive/24_series/24.301/.

[5] 3GPP, S1 Application Protocol (S1AP), Tech. Rep. 3GPP TS 36.413 v0.0.0, 3rd Generation Partnership Project-3GPP, 2008, https://www.3gpp.org/ftp/Specs/archive/36_series/36.413/.

[6] 3GPP: System architecture for the 5g system (5gs). Technical Specifcation (TS) 23.501, 3rd Generation Partnership Project (3GPP) (2019). Version 16.0.0

[7] R.D. Kaliski, Heterogeneous network architecture and device-to-device communications in 5G cellular networks. Wiley 5G Ref: The Essential 5G Reference Online, pp. 1–24 (2019)

[8] 3GPP: Non-access-stratum (nas) functions related to mobile station (ms) in idle mode. Technical Specifcation (TS) 23.122, 3rd Generation Partnership Project (3GPP) (2020). Version 17.0.0

[9] 3GPP: Evolved universal terrestrial radio access (e-utra); user equipment (ue) procedures in idle mode. Technical Specifcation (TS) 36.304, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0

[10] 3GPP: Evolved universal terrestrial radio access (E-UTRA); requirements for support of radio resource management. Technical Report 36.133, 3rd Generation Partnership Project (3GPP) (2019). Version 16.0.0

[11] 3GPP: Evolved universal terrestrial radio access (E-UTRA); radio resource control (RRC); protocol specifcation. Technical Report 36.133, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0 [12] G.J. Myers, C. Sandler, T. Badgett, The Art of Software Testing, third ed., Wiley Publishing, 2011, URL https://dl.acm.org/doi/book/10.5555/2161638.

[13] 3GPP, 5G; System architecture for the 5G system (5GS), 2020, URL https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf.

[14] J. Meredith, M. Pope, 3rd Generation Partnership Project Technical Specification Group Services and Systems Aspects Release 15 Description, Tech. Rep. 3GPP TR21.915 V15.9.0, 3rd Generation Partnership Project-3GPP, Sophia Antipolis CEDEX, France, 2018, https://www.3gpp.org/ftp/Specs/archive/21_series/21915/.

[15] K.V. Cardoso, C.B. Both, L.R. Prade, C.J. Macedo, V.H.L. Lopes, A softwarized perspective of the 5G networks, 2020, CoRR abs/2006.10409, arXiv:2006.10409. URL https://arxiv.org/abs/2006.10409.

[16] P. Hedman, et al., 5G Core Networks: Powering Digitization, first ed., vol. 1, Elsevier Science & Technology, United Kingdom, 2019, http://dx.doi.org/10.1016/C2018-0-01335-3.

[17] 3GPP, Non-Access-Stratum (NAS) Protocol for 5G System (5GS), Tech. Rep. 3GPP TS 24.501 V16.5.1, 3rd Generation Partnership Project-3GPP, 2020, https://www.3gpp.org/ftp/Specs/archive/24_series/24.501/.

[18] 3GPP, NG Application Protocol (NGAP), Tech. Rep. 3GPP TS 38.413 V16.2.0, 3rd Generation Partnership Project-3GPP, Sophia Antipolis CEDEX, France, 2020,
https://www.3gpp.org/ftp/Specs/archive/38_series/38.413/.

[19] M. Burrows, M. Abadi, R. M. Needham, A logic of authentication, Proceedings of the Royal Society of
London. A. Mathematical and Physical Sciences, Vol. 426, No. 1871, pp. 233-271, Dec. 1989.

[20] C. J. F. Cremers, The Scyther Tool: Verification, falsification, and analysis of security protocols, International conference on computer aided verification, Princeton, NJ, USA, 2008, pp. 414-418.

[21] A. DeKok, The Network Access Identifier, IETF RFC 7542, May, 2015.

[22] C. Boyd, W. Mao, On a limitation of BAN logic, Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, 1993, pp.240-247.

[23] C. A. Meadows, Formal verification of cryptographic protocols: A survey, International Conference on the Theory and Application of Cryptology (ASIACRYOPT), Wollongong, Australia, 1994, pp. 133-150.

[24] J. Arkko, H. Haverinen, Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA), IETF RFC 4187, January, 2006.

[25] J. Arkko, V. Lehtovirta, P. Eronen, Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'), IETF RFC 5448. May, 2009.

[26] G. Brown, New transport network architecture for 5G RAN, Fujitsu, Kanagawa, Japan, White Paper, 2018.

[27] Samsung, 4G-5G Interworking: RAN-Level CN-Level Interworking, June, 2017.