IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE VEHICULAR TECHNOLOGY SOCIETY SECTION

Received August 3, 2021, accepted August 14, 2021, date of publication August 24, 2021, date of current version September 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3107308

A Formally Verified Security Scheme for Inter-gNB-DU Handover in 5G Vehicle-to-Everything

JIYOON KIM[1], (Student Member, IEEE), DANIEL GERBI DUGUMA[1], PHILIP VIRGIL ASTILLO[1], HOON-YONG PARK[1], BONAM KIM[1], ILSUN YOU[1], (Senior Member, IEEE), AND VISHAL SHARMA[2], (Senior Member, IEEE)

[1]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea
[2]School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast (QUB), Belfast BT7 1NN, Northern Ireland, U.K.

Corresponding author: Ilsun You (ilsunu@gmail.com)

This work was supported in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) Grant by the Korean Government through Ministry of Science and ICT (MSIT) (Development of 5G Edge Security Technology for Ensuring 5GC Service Stability and Availability, 95%) under Grant 2020-0-00952, and in part by Soonchunhyang University Research Fund (5%).

ABSTRACT Cellular technology has evolved over the decades for mobile network operators to accommodate the ever-growing demands of services for connecting Vehicle-to-Everything (V2X). The 5G infrastructure facilitates V2X communications, where a small-cell base station operating at ultra-high radio frequency with limited coverage becomes pervasive. These small-cell base stations in 5G-V2X must be strategically deployed near the consumers to realize several use cases. More recently, the architectural split solutions in Next Generation Radio Access Network (NG-RAN) are introduced, in which the gNB is divided into the distributed unit (gNB-DU) and control unit (gNB-CU). This functional split intends to improve scalability, performance, and network orchestration optimization. In this case, frequent user equipment (UE) handover between gNB-DUs is inevitable. However, the current 5G standard did not consider securing the path between these two entities. Hence, the NG-RAN could likely experience various security threats if the current handover procedure standard is employed without changes. Consequently, this paper introduces potential threats like resource depletion at NG-RAN caused by the useless execution of resource-demanding procedures to complete the transfer of attachment of UE to target gNB-DU. Another is UE being denied from accessing services caused by unsuccessful uplink and downlink synchronization during random access procedure execution, requiring establishing security and mutual authentication between the entities. Motivated by this, we proposed a security protocol composed of two phases, namely initial and handover. While the former phase assists in mutual authentication and key agreement between UE and serving gNB-DU, the latter secures UE's mobility in inter-gNB-DU handover. This protocol aims to preserve the existing quality of service and support essential security requirements, including confidentiality, integrity, mutual authentication, secure key exchange, and perfect forward secrecy. The security requirements are formally verified using BAN logic and Scyther, and the proposed protocol demonstrated lower handover latency than EAP-AKA', AKA, EAP-TLS, and EAP-IKEv2.

INDEX TERMS NG-RAN, inter-gNB-DU handover, mobility management security, formal verification.

I. INTRODUCTION

The advancement of 5G technology compels the transition of broadband networks from vertical to horizontal systems, thereby supporting real-time communications in vehicular networks [1]. The current structure, which combines multiple devices and ultra-high-density wireless components, attempts to manage communication in a small network. Consumers (vehicles) will increasingly discover the core offerings such as eMBB (enhanced Mobile Broadband), URLLC (Ultra-Reliable & Low Latency Communications), and mMTC (massive Machine-Type Communications) under

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Quan.

this new arrangement [2]. Despite the significant values delivered to the vehicles and service providers, the technology brought new security challenges to the vehicular communication ecosystem. The 3GPP TS 33.809, for instance, warns about the critical vulnerabilities and attacks in the messages used in 5G networks, especially in the NG-RAN [3]. These have a severe impact when high mobility environments similar to vehicular networks are involved. The high throughput and efficient reuse of spectrum in 5G networks are satisfied by small cell technology that uses millimetre-wave signals. Yet, such a reduction in cell size introduced frequent handover and traffic overheads.

Vehicular communication is seen as one of the most prominent 5G application areas that have attained a lot of attention in recent years, specifically focusing on security and efficiency [4]. In such applications, the network that provides the communication mechanisms for Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Pedestrian (V2P), and in general, Vehicle-to-Everything (V2X) needs to satisfy the URLLC requirement offered by the 5G mobile network [5] [6], [7]. Furthermore, due to their high mobility (often with high speed), vehicles and the passengers posing as a piece of User Equipment (UE) perform repeated handovers assisted through the gNB.

The functional split introduced in the Next-Generation Radio Access Network (NG-RAN) divides the gNB into Control Unit (gNB-CU), Distributed Unit (gNB-DU), and Radio Unit (gNB-RU). The gNB-CU typically resides at a moderately higher level relative to vehicles acting as UE and next to gNB-DU and gNB-RU. In such setups, while gNB-CU manages the Radio Resource Control (RRC), Service Data Association Protocol (SDAP), and Packet Data Convergence Protocol (PDCP) protocols, the gNB-DU processes Radio Link Control (RLC), Media Access Control (MAC), and Physical (PHY) layer services [8]. Concerning the location of these components, this paper considers the placement of gNB-DU and gNB-RU distributed at the cell site and the gNB-CU centralized at the far edge for supporting smooth vehicular handovers [9].

The disaggregation of NG-RAN, apart from increased flexibility and improved performance, has introduced different handover techniques such as inter-gNB-CU and inter-gNB-DU applicable to 5G-V2X. The former method transfers a UE from a source gNB-CU to a destination gNB-CU over an Xn interface. However, it is inefficient (despite the secure channel UE establishes with gNB-CU over RRC setup) for the gNB-CU, which is relatively far from the user, to manage and control the UE's communication. Although it is more desirable to process the network control through the gNB-DU as specified in the inter-gNB-DU handover technique, the signaling messages transmitted between the UE and the gNB-DU are not protected. Consequently, this exposes the messages to different security threats [10], [11].

In this paper, the focus is on location and route management for veicular communications. The prior is involved in mutual authentication between the UE (vehicles) and the 5G network. At the same time, it confirms whether the UE is connected or not. On the other hand, the route management provides an efficient communication environment by reconfiguring the network path according to the location of the UE [12]. Furthermore, in design decisions where the gNB-DU only transmits the control messages to and from the gNB-CU in the communication between the UE and the 5G core, a mismatch may result between the intended location and the actual location of UE. This deviation can, in turn, cause fatal flaws such as network resource depletion and relay attacks [13]. As a result, it is vital to deploy security mechanisms to protect the vehicular mobility in the inter-gNB-DU handover scenarios. An exemplary illustration of the inter-gNB-DU handover scenario for vehicular communications in 5G is shown in Figure 1.

Motivated by this, we propose a new security protocol for inter-gNB-DU handover consisting of the initial and handover phases in 5G-V2X. In the former, the UE and the gNB-DU rely on the trust extablished in the 5G primary authentication to perform mutural authentication and negotiate a strong master session key. The negotiated key is then used in the latter to protect inter-gNB-DU handover and update itself newly. In this way, the proposed protocol not only enforces access control to ensure that legitimate vehicles are allowed to enter the gNB-DU's cell, but also establishes the secure channel betweem the UE and the gNB-DU to protect their communication. Thereby, it can address various security threstes existing in the path between the UE and the gNB-DU such as the false base station (FBS) attacks reported by [3].

The main contributions of this paper are summarized as follows:

- Designing a security protocol (known as Initial Phase) to establish mutual authentication and construct a secure channel between the UE (vehicles) and the gNB-DU by deriving a master session key for the handover phase.
- Designing a security protocol for the inter-gNB-DU handover that enables a UE to move between gNB-DUs securely.
- Formally verifying the proposed protocols and comparing them with well-known security protocols in tems of security and efficiency.

The rest of the paper is structured as follows: Section 2 puts forward the background for the 5G handover, particularly the inter-gNB-DU handover and its potential threats. Section 3 gives the details of the proposed protocol, and section 4 provides its formal verification. The final two sections describe the comparison of the proposed protocol against the existing protocols and the paper's conclusion, respectively.

II. RELATED WORKS

In this section, we provide a background for secure communication of UE and gNB-DU by first describing the NG-RAN, then presenting the inter-gNB-DU handover, and finally pointing out the potential security threats.

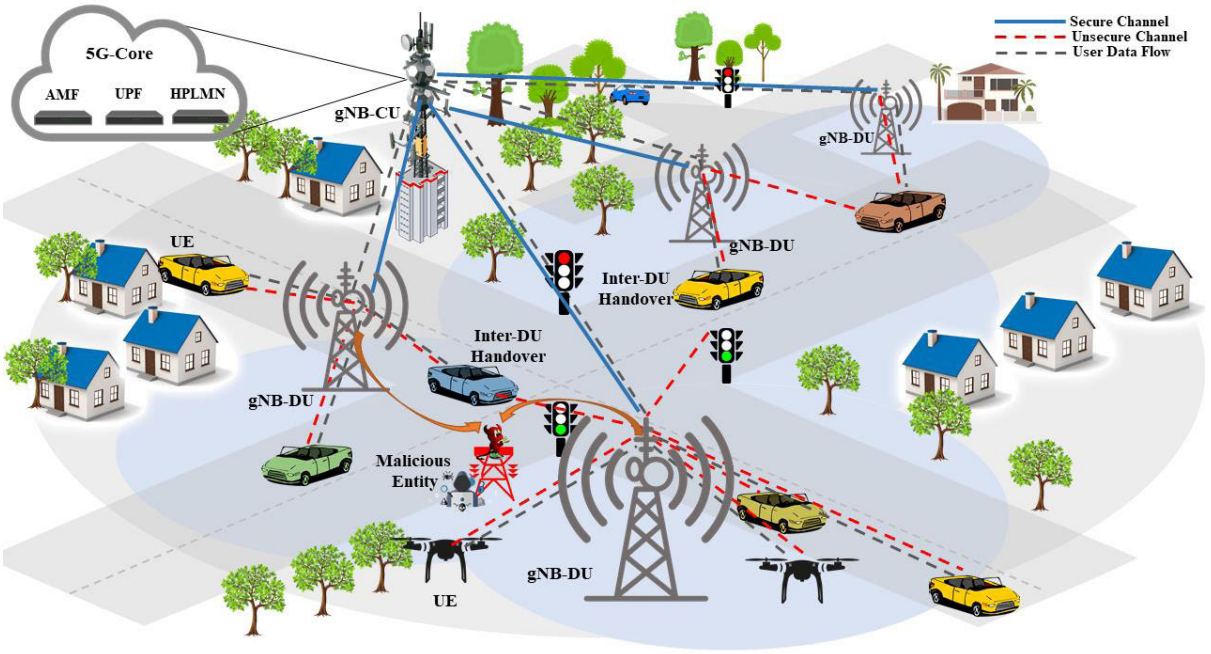


FIGURE 1. An exemplary illustration of the inter-gNB-DU handover scenario for vehicular communications.

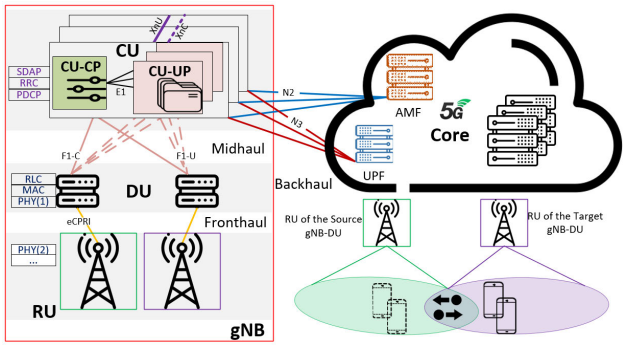


FIGURE 2. The architecture of NG-RAN.

A. NG-RAN

The NG-RAN architecture, unlike its predecessors, shadows a new design that leverages functional splitting for fine-grained decisions and control of resources. The architecture, as depicted in Figure 2, divides gNB functions into gNB-CU, gNB-DU, and gNB-RU, which connect with the 5G core (5GC) – specifically to AMF (Access and Mobility Functions) through N2/NG-C interface and UPF (User Plane Function) via N3/NG-U interface. The further division of gNB-CU results in the control plane (CU-CP) and the user plane (CU-UP) components interacting via an E1 interface. The CU-CP handles protocols such as SDAP, RRC, and PDCP with an F1-C interface in the mid-haul. The user plane part of these protocols, along with the F1-U mid-haul interface, is handled by CU-UP. F1 is a newly introduced interface in NG-RAN that allows exchanging data (via F1-U) and signaling information (via F1-C) between gNB-CU and gNB-DU while separating the radio and transport layers. F1-C is responsible for gNB-CU and gNB-DU configuration management, F1 interface setup and operation, error controlling, UE context management functions, etc. The F1-U, on the other hand, handles flow control and user data transfers [14].

Besides the intra-gNB communication (inter-action between gNB-CU and gNB-DU), inter-communication between two gNBs, particularly between gNB-CUs, is carried out using an Xn interface (Xn-U and Xn-C) corresponding to CU-UP and CU-CP, resp. The gNB-DU handles the lower protocol stacks. They also communicate with the gNB-RUs via different interfaces, most likely using an eCPRI (enhanced Common Public Radio Interface) in the front-haul network. While the gNB-RU is responsible for 'raw' radio actions, such as Tx/Rx and ADC, gNB-DU takes care of the digital processing of information, among others. In addition, the functional separation of gNBs into gNB-CUs and gNB-DUs can also satisfy service-friendly requirements such as transport network capacity and latency. Such split applies not only to gNBs but also to signaling messages for each layer. In more detail, while a gNB-CU controls the signaling messages of the RRC and PDCP layers, a gNB-DU handles the MAC and RLC layers.

It is worth noting that gNB-DU, unlike gNB-CU, cannot establish a secure channel with UE. Consequently, the signaling messages exchanged between gNB-DU and UE can be exposed to security threats, enabling attackers to overwhelm the gNB-CU with massive processing requests via gNB-DU. This paper focuses on the inter-gNB-DU handover, which requires the gNB-CU to carry the accompanying signaling overhead, resulting in a traffic bottleneck [15].

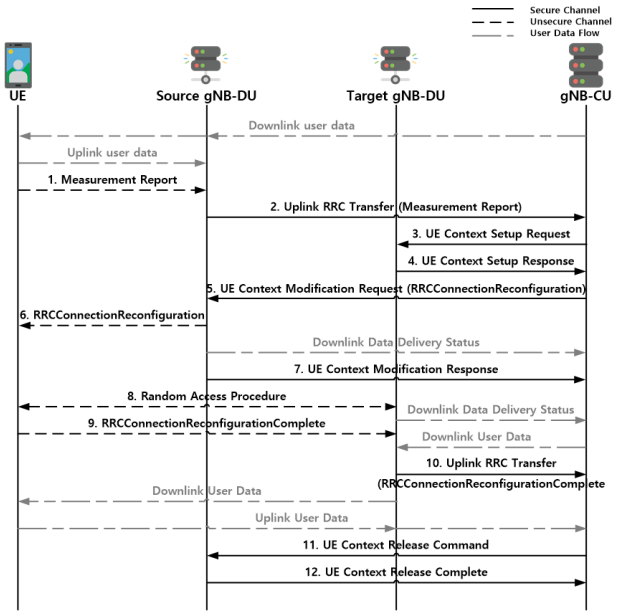


FIGURE 3. The procedure of the inter-gNB-DU handover.

B. INTER-GNB-DU HANDOVER AND POTENTIAL THREATS ANALYSIS

According to the NG-RAN handover procedure outlined by the 3GPP in [8], a seamless handover is required when a UE transfers connection to another gNB-DUs, in which source and destination gNB-DUs are under a single gNB-CU. This scenario is commonly known as inter-gNB-DU handover. In this section, we focus on inter-gNB-DU Mobility Management, an NG-RAN handover procedure of [8]. In the inter-gNB-DU handover shown in Figure 3, the gNB-DU only plays the role of a bearer in the communication between the UE and the gNB-CU

Meanwhile, one critical issue observed in the current handover procedure is the absence of mutual authentication and a secure channel between the UE and the gNB-DU. Therefore, regardless of the access authority, some possible security incidents could likely happen if the current handover management mechanism is employed. Consequently, this section introduces the inter-gNB-DU handover procedure, including an initial analysis of possible threats that must be resolved.

According to [8], the inter-gNB-DU handover, shown in Figure 3, is covered by the initial registration's RRC and AS setup. The UE sends the current state to the source gNB-DU via the Measurement Report (MR), which the source gNB-DU encodes with an Uplink RRC Transfer message and sends to the gNB-CU. However, at this point, the UE can freely send the MR without authentication to the source gNB-DU. This means that, as depicted in Figure 4, a malicious UE can send valid dummy reports to cause the source gNB-DU, target gNB-DU, and gNB-CU to be uselessly occupied with the subsequent resource-demanding steps, thereby depleting their resources.

Upon reception of UE's MR, the gNB-CU subsequently decides whether to execute the handover. Under such circumstances, it prepares the target gNB-DU for handover through the UE Context Setup Request message. When the planning is over, the target gNB-DU sends the UE Context Adjustment Request to the source gNB-DU for UE context modification. Proceeding to RRC link reconfiguration, the source gNB-DU sends the RRCConnectionReconfiguration message together with the UE Context Modification Request message to the UE. The gNB-DU informs the gNB-CU of the situation following the request through the UE Context Modification Response message.

When the UE connects to the target gNB-DU, the Random Access (RA) Procedure begins. This protocol is intended to synchronize uplink and downlink sessions and reestablish the RRC connection with the network. However, possible threats can also be observed during this phase, as illustrated in Figures 5 and 6. Considering Contention-based Random Access, multiple UEs compete to establish synchronization through sending a randomly selected preamble from the shared pool of preambles; thereby, collisions can likely be experienced by UEs, resulting in a delay of successful synchronization. Unfortunately, such a situation can be exploited by sophisticated UE-acting attackers continuously transmitting preambles, as illustrated in Figure 5, which could lead to denial of service attacks if the RA request message is not authenticated. In addition, legitimate UE could be associated with a False base station, as presented in Figure 6, if the RA response is not warranted, leading to UE's inability to access services from the genuine network.

Furthermore, after successful downlink and uplink synchronization with the network, UE sends the RRCConnectionReconfigurationComplete message to the target gNB-DU. The RRCConnectionReconfiguration-Complete message is encoded by the Uplink RRC Transfer and forwarded to the gNB-CU by the target gNB-DU. The gNB-DU is aware of the RRC relation reconfiguration between the UE and the Target gNB-DU via Uplink RRC Transfer and sends the UE Context Release Command message to the source gNB-DU to recover the resources allocated to the UE. The source gNB-DU releases the assigned resources and sends the UE Context Release Complete message to the gNB-CU. Such release event of UE indicates its successful handover to the target gNB-DU.

The identified vulnerabilities of the current inter-gNB-DU handover procedure must be further studied to establish more substantial evidence that it can be exploited to launch a more harmful attack. In spite of that, those initially identified threats are theoretically doable considering the continuous advancement of tools and equipment (e.g., software-defined radio (SDR)) that are sometimes utilized for malicious purposes. Therefore, this initial analysis motivates this paper to secure the inter-gNB-DU handover protocol while addressing the identified threats.

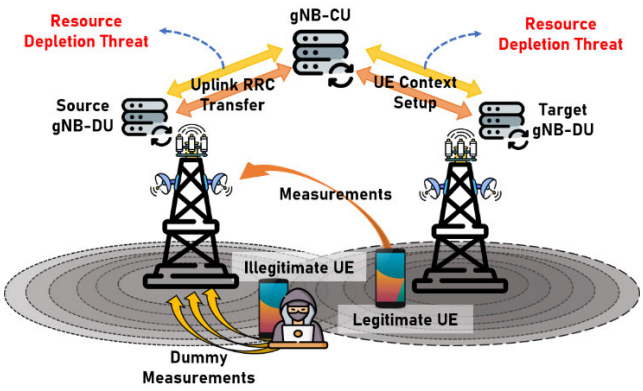


FIGURE 4. Potential threat of unauthenticated MR.

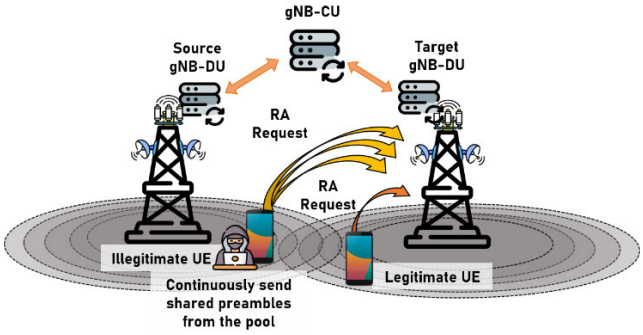


FIGURE 5. Potential threat of unauthenticated RA request.

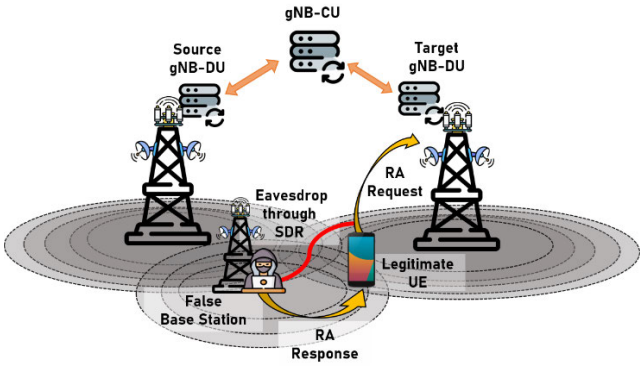


FIGURE 6. Potential threat of unauthenticated RA response.

III. PROPOSED PROTOCOL

This section presents an inter-gNB-DU handover security protocol. The proposed protocol consists of two phases: Initial phase and Handover phase. The target environment of the proposed protocol is composed of UE, source gNB-DU, target gNB-DU, gNB-CU, and AMF. First, the mutual authentication and key exchange between the UE and gNB-DU is carried out using the initial phase security protocol, which is conducted based on the UE Initial Access Procedure [8]. Next, the handover phase protocol proceeds by securing the channel between the UE and the source gNB-DU through the master secret key communicated in the initial phase. Subsequently, the UE is securely attached to the target gNB-DU by leveraging the session key *SK* derived from the pre-wise master key transferred from the gNB-CU.

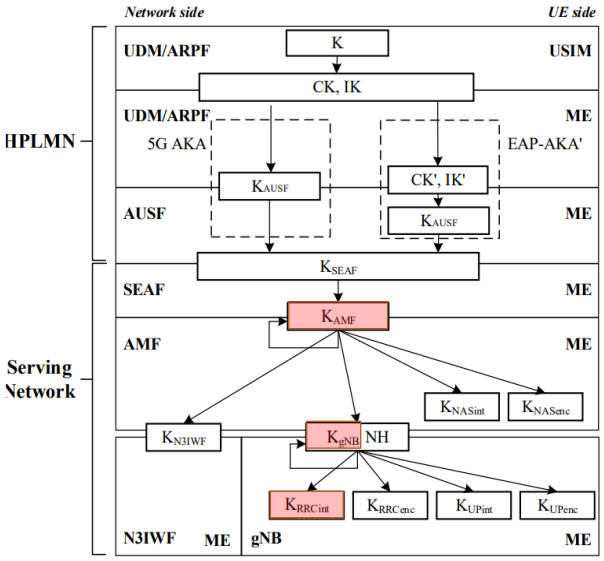


FIGURE 7. Key hierarchy generation in 5G.

A. THE 5G KEY HIERARCHY

In 5G, a UE and its core network pre-share the long-term key K, which serves to derive all session keys. These derivations form a key hierarchy used to secure the communication between the UE and the 5G system and among the network functions in this system. After successful primary authentication (via 5G AKA [16] or EAP-AKA' [17]), the UE and the core network compute K_{SEAF}. Next, K_{AMF} is derived and then used to obtain the confidentiality and integrity (K_{NASint} and K_{NASenc}) keys for NAS signaling. The same key also assists in the derivation of the K_{gNB} and K_{N3IWF}. Finally, the UE and its corresponding gNB use the former key to calculate the AS confidentiality and integrity signaling keys (K_{UPint} and K_{UPenc} for user plane and K_{RRCint} and K_{RRCenc} for control plane) to protect the traffic between them. Figure 7 shows the key hierarchy procedure, with K_{AMF}, K_{gNB}, and K_{RRCint} highlighted in red. The proposed protocol uses these three keys to derive different keys, such as *MSK* (Master Key) in the initial phase and *PMSK* (Pre-wise Master Key) in the handover phase.

B. ELLIPTIC CURVE DIFFIE-HELLMAN KEY EXCHANGE

Elliptic curve cryptography (ECC) is an efficient public-key cryptography scheme that provides similar security to other public-key algorithms while requiring less key size and memory requirements [18]. Based on ECC, the elliptic curve Diffie-Hellman (ECDH) key exchange can provide a relatively efficient public-key exchange between the UE and the gNB-DU. Unlike ECDH having a static public key, ECDHE (ECDH Ephemeral) uses an ephemeral public key and can support perfect forward secrecy. To proceed with ECDHE, the UE and the gNB-DU share the domain

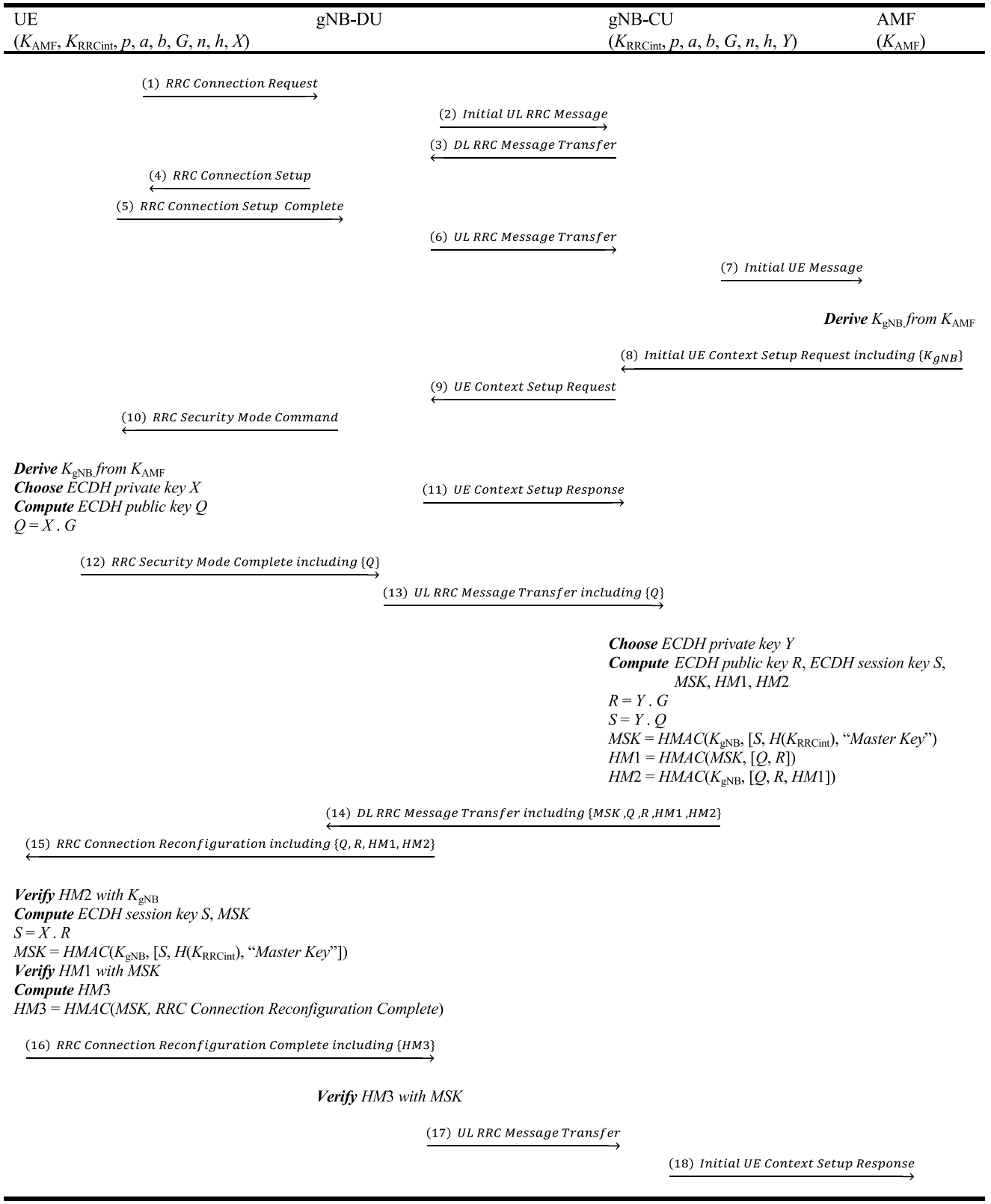


FIGURE 8. The initial phase of the proposed protocol (init phase).

parameters ahead of time and use these parameters to generates a short-lived key pair and exchanges the public keys with one another. This process is shown in Table 1.

It is important to note that a secure distribution of the public keys is needed to protect the communication from attacks such as man-in-the-middle. Consequently, our protocol uses

TABLE 1. Elliptic curve Diffie-Hellman key exchange.

ECDHE Key Generation and Exchange Algorithm

Requirement: The domain parameters $(p, a, b, G, n, and\ h)$* are agreed and known by both UE and gNB-DU.

I. Generating the private and public keys

1. UE chooses a random integer X from {1, …, n-1} as its ephemeral private key.
2. UE computes its ephemeral public key Q using the elliptic curve scalar multiplication: $$Q = X \,.\, G.$$
3. gNB-CU/gNB-DU chooses a random integer Y from {1, …, n-1} as its ephemeral private key.
4. gNB-CU/gNB-DU computes its ephemeral public key R using the elliptic curve scalar multiplication: $$R = Y \,.\, G.$$

II. Exchanging the public keys

5. UE sends its public key Q to gNB-CU/gNB-DU.
6. gNB-CU/gNB-DU sends its public key R to UE.

III. Computing the shared key

7. UE computes the shared key S: $$S = X \,.\, R = X \,.\, Y \,.\, G$$
8. gNB-CU/gNB-DU computes the shared key S: $$S = Y \,.\, Q = Y \,.\, X \,.\, G$$

p: a prime number indicating the size of the finite field.
a, b: the coefficients for the chosen elliptic curve equation.
G: the base point to generate a subgroup.
n, h: the order and cofactor of the subgroup, respectively.

a secure line to deliver the ephemeral public keys of UE and gNB-CU (in the initial phase) and UE and the target gNB-DU (in the handover phase), as illustrated in Figure 8 and Figure 9, respectively. In the initial phase, the UE sends its public key via the *RRC Security Mode Complete* and *UL RRC Message Transfer* messages and receives the gNB-CU's ephemeral public key over the *DL RRC Message Transfer* and *RRC Connection Reconfiguration* messages. In the handover phase also, UE and the target gNB-DU exchange their public keys through Random Access Request and Random-Access Response messages. Hence, using the ECDHE, the session keys computed by the UE and gNB-CU/gNB-DU satisfy the perfect forward secrecy while alleviating the man-in-the-middle attack.

C. THREAT MODEL

Security protocols designed to operate in open environments, such as the one we proposed in this paper, often face various challenges. For example, attackers can obtain sensitive information by capturing data from either encrypted or plaintext messages transmitted over the air. Consequently, it is essential to model these protocols' environments to clearly understand how they operate in the presence of an adversary and yet deliver the required service without interruption. One of the most common methods used prevalently for this purpose is the Dolev-Yao (DY) threat model [19].

The DY paradigm assumes an unreliable open channel that renders interacting actors treacherous. The adversaries in this model are regarded as most powerful as they can intercept network communications to initiate and receive malicious data by aping the authentic entities. However, this does not allow these attackers to decipher/encipher the encrypted/plain messages, assuming that the encryption mechanism is provably secure. In addition, attackers cannot extract hashed messages or accurately guess the random nonce used in the security system unless they acquire the correct keys within the acceptable time frame.

The main intention of designing a security protocol that operates in such an environment is to enable communicating parties to establish a secure channel despite the existence of an intruder. In our proposed protocol, the communication between a UE and its core network passes through a public channel that lets the DY attacker manipulate the messages conveying. Hence, given the proposed protocol's operating characteristics, it can be best represented using the DY threat model. That is, our protocol serves to create a secure channel between the UE and the gNB-DU by assuring confidentiality, integrity, mutual authentication, secure key exchange, and perfect forward secrecy requirements for safe service delivery (as proved in section IV).

D. SECURITY REQUIREMENTS

As 5G network environments use ultra-high frequencies, the cell size is reduced compared to the previous generation. It means that the user equipment must proceed with handovers frequently due to the reduced cell size. In addition, the traffic handled by the network has dramatically increased because of the various and the massive number of devices accessing the network. In such situations, the MR essentially included in the handover can be exposed to threats whenever the UE tries to transfer the connection. Thus, a handover protocol that can maintain the existing quality of service is required while securing the reliability and availability of the users and networks. For this, the proposed protocol should satisfy several requirements.

Primarily, the proposed protocol should provide confidentiality, which means that the unauthorized participant cannot access the secret key (e.g., *MSK, SK*). By confidentiality, the secret key between UE and gNB-DU can guarantee the communication partner. In addition, the identified potential threats of the current inter-gNB-DU handover standard are deduced from the unverified validity of the messages between UE and gNB-DU. Thus, the proposed protocol should provide the means to verify the authenticity of the messages between the two entities. Moreover, mutual authentication is a proven effective measure of ensuring the legitimacy between two communicating entities. In other words, it prevents both legitimate UE and gNB-DU from being misled by UE-acting or gNB-DU-acting adversaries in performing subsequent useless operations.

Furthermore, UE should share a mutually agreed secret key with gNB-DU to establish a secure channel, supporting

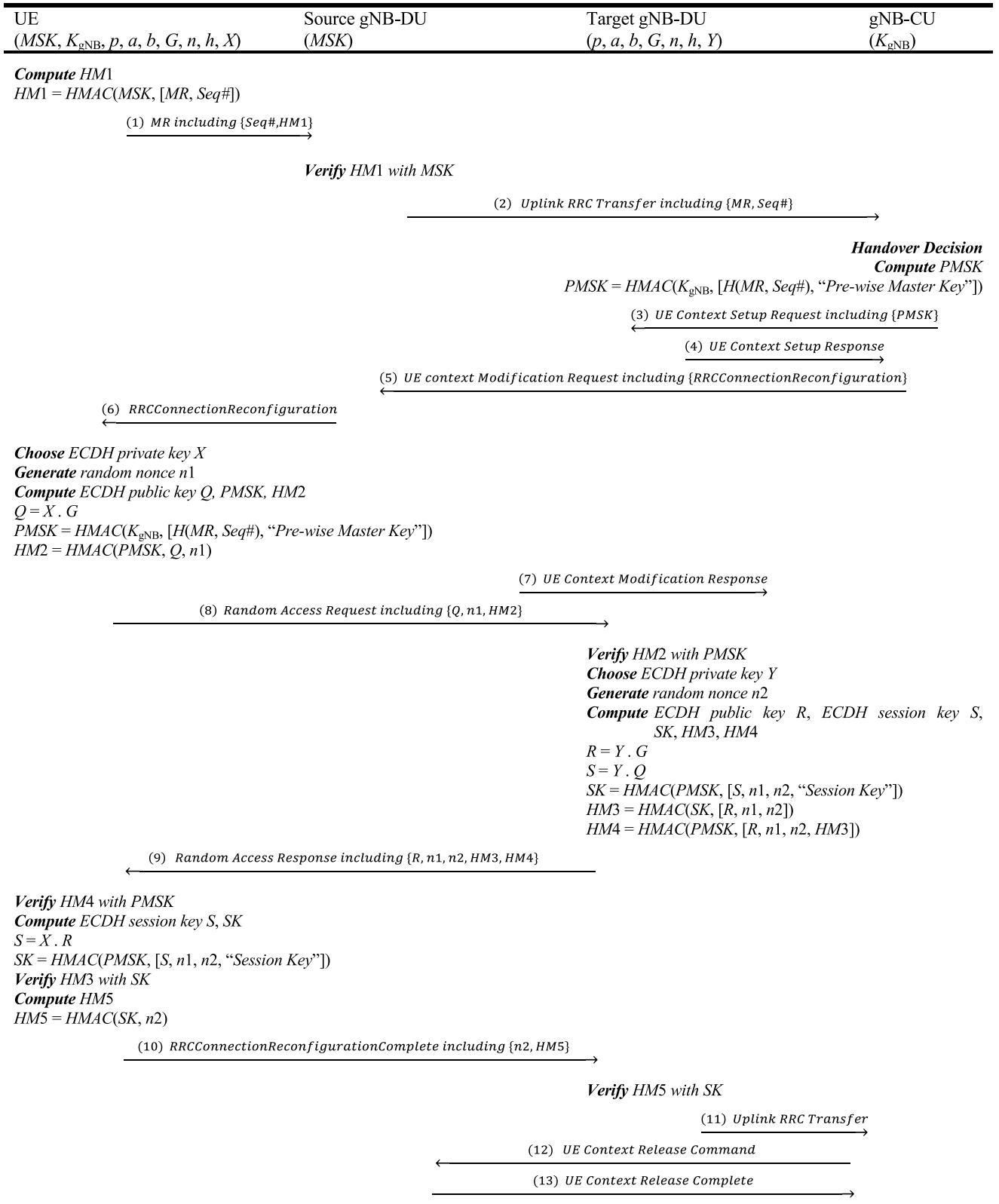


FIGURE 9. The handover phase of the proposed protocol (HO phase).

confidentiality and integrity requirements. Finally, in an environment where frequent handover is inevitable, the secret keys (i.e., session key) between sessions must be independent. In more precisely, even if the past keys are leaked, the

TABLE 2. Notations.

Notation	Description
UE	User equipment
gNB-DU	Distributed unit of the gNB
gNB-CU	Control unit of the gNB
ECDH	Elliptic Curve Diffie-Hellman
MSK	Master key between the UE and the gNB-CU
PMSK	Pre-wise MSK
SK	Session Key between the UE and the gNB-DU
X, *Y*	ECDH private keys
Q, *R*	ECDH public keys
S	ECDH session key
*n*x	x-th nonce
Seq#	Sequence number
HMAC	Hash-based message authentication code

communication channel between UE and gNB-DU should be still secure since previous keys have strongly no correlation with the keys in the subsequent sessions.

Accordingly, the proposed protocol should satisfy the following security requirements to make it stand against various security attacks:

1. **Confidentiality**: An attacker should not be able to reveal the secret key transmitted between the UE and the gNB-DU.
2. **Integrity**: An intruder should not be able to modify the signaling messages transmitting between the UE and the gNB-DU.
3. **Mutual Authentication**: The UE should authenticate the gNB-DU to prevent malicious attacks by FBS. The gNB-DU should also verify the UE to avoid false MR and location spoofing.
4. **Key Exchange**: The keys used to secure the communication between the UE and the gNB-DU should be securely negotiated.
5. **Perfect Forward Secrecy**: The current session keys used by UE and gNB-DU should not be derived through the past session keys.

E. NOTATIONS

The notations used in the proposed protocol are defined as Table 2.

F. INITIAL PHASE

As shown in Figure 8, this phase of the protocol dictates the preliminary steps that the UE and the gNB-DU requires. The most important of these are mutual authentication and establishing a secure channel between them before data communication and handover. That is even vital concerning gNB-DU as it cannot derive the master key *MSK* since there is no pre-shared information between the UE and itself. Hence, the initial phase is designed to securely exchange the master key *MSK* between the UE and the gNB-DU with the assistance of gNB-CU. Note that the UE and the gNB-CU share the secure key K_{gNB} that is derived from K_{AMF} as secret information for generating the master key *MSK*.

As presented in the Figure 8, the protocol leverages ECDHE key exchange and randomly generated nonce for perfect forward secrecy and mutual authentication. The details of the message exchanges of the initial phase of the protocol are described as follows:

Steps 1-7: These steps follow the RRC initial connection procedure in 3GPP TS 38.401.

Step 8: The AMF derives K_{gNB} from K_{AMF} according to the key hierarchy and sends the K_{gNB} as part of the initial UE Context Setup Request message to the gNB-CU.

Steps 9-11: These steps follow the RRC initial connection procedure in 3GPP TS 38.401.

Step 12: Upon receiving the RRC Security Mode Command message, the UE derives K_{gNB} from K_{AMF} and generates the ECDH private key *X* and calculates the ECDH public key *Q*. The UE then sends the RRC Security Mode Complete message (that includes ECDH public key *Q*) to the gNB-DU.

Step 13: The gNB-DU encodes the RRC Security Mode Complete message to the UL RRC Message Transfer and transmits it to the gNB-CU.

Step 14: When the gNB-CU receives the UL RRC Message Transfer, it generates the ECDH private key *Y* and the ECDH public key *R*. The ECDH session key *S* is then computed from the UE's ECDH public key *Q* and its own ECDH private key *Y*. The master session key *MSK* is derived through K_{RRCint} (the integrity key used in RRC communication between the UE and the gNB-CU), K_{gNB} (delivered from the AMF), and the session key *S*. The gNB-CU then creates the message authentication codes (*HM*1 and *HM*2) with K_{gNB} and *MSK* to protect the message and prove the possession of the key, respectively. Finally, the gNB-CU sends the DL RRC Message Transfer containing *MSK, R, HM1 and HM2* to gNB-DU.

Step 15: The gNB-DU stores the *MSK* from the DL RRC Message Transfer and transmits the RRC Connection Reconfiguration message to the UE including *R, HM1 and HM2*.

Step 16: The UE receiving the previous message first verifies the message authentication code *HM*2 with K_{gNB}. For a positive result, it derives the ECDH session key *S* and the master key *MSK* with its ECDH private key *X* and the gNB-CU's ECDH public key *R*. Next, the UE verifies *HM*1 using the derived master key *MSK*. If *HM*1 is valid, the UE then generates the message authentication code *HM*3 with the master key *MSK*, which is used to protect the RRC Connection Reconfiguration Complete message, and transmits it to the gNB-DU.

Step 17: The gNB-DU verifies the message authentication code *HM*3 with the master key *MSK*. If *HM*3 is valid, it assures both UE and gNB-DU about the safe exchange of the master key. Next, the gNB-DU encodes the RRC

Connection Reconfiguration Complete message to the UL RRC Message Transfer and sends it to the gNB-CU.

Step 18: As the final point of the initial phase, the gNB-CU transmits the Initial UE Context Setup Response message to the AMF to notify that the initial phase is complete.

G. HANDOVER PHASE

Once the initial phase of the protocol completes successfully and that both gNB-DU and UE possess the maser key *MSK*, the handover phase of the protocol proceeds. In particular to this protocol, the UE is regarded as a mobile that can move between gNB-DUs. In this scenario, the gNB-CU decides the handover and transfers the pre-wise master key *PMSK* to the target gNB-DU. The target gNB-DU then derives the session key *SK* from the pre-wise master key *PMSK*. Figure 9 shows the handover phase of the proposed protocol, and the details of the message flow described as follows:

Step 1: The UE records the status of the current network and the devices from the *MR*. The UE then generates the message authentication code *HM*1 with the *MR*, the sequence number *Seq*#, and the master key *MSK* and then transmits it to the source gNB-DU.

Step 2: The source gNB-DU verifies the message authentication code *HM*1 with the master key *MSK* and checks the sequence number *Seq*#. If the *HM*1 and the *Seq*# are valid, the source gNB-DU encodes the *MR* to the Uplink RRC Transfer message and sends it to the gNB-CU.

Step 3: Once the Uplink RRC Transfer message reaches the gNB-CU, it checks the received *MR* and decides the handover. When the handover is determined, the gNB-CU derives the pre-wise master key *PMSK* with the secret key K_{gNB} and the hash value of the *MR*. Next, it transmits the *PMSK* to the target gNB-DU through a secure channel.

Step 4: The target gNB-DU stores the *PMSK* and passes on the UE Context Setup Response message to the gNB-CU.

Step 5: Upon receiving the UE Context Setup Response message, the gNB-CU transmits the UE Context Modification Request message to the source gNB-DU.

Steps 6-7: The source gNB-DU extracts the RRC-ConnectionReconfiguration message from the UE context Modification Request message and transmits it to the UE. After transmission, the source gNB-DU sends the UE Context Modification Response message to the gNB-CU.

Step 8: When the RRCConnectionReconfiguration message reaches UE, the UE derives the *PMSK* with K_{gNB} and generates the ECDH private key X, the ECDH public key Q, and randomly generated nonce $n1$. In addition, *PMSK*, Q, and $n1$ are used to form the message authentication code *HM*2. The UE then constructs the Random Access Request message, including Q, $n1$, and *HM*2. Finally, the target gNB-DU receives this message.

Step 9: As soon as the previous message hits the target gNB-DU, it verifies the *HM*2 with *PMSK*. If *HM*2 is valid, then the target gNB-DU can confirm that the UE has requested handover to the gNB-CU. Subsequently, the target gNB-DU generates the ECDH private key Y, the ECDH public key R, and random nonce $n2$. Next, the target gNB-DU computes the ECDH session key S using its private key Y and the UE's public key Q. Also, the target gNB-DU generates the session key *SK* using *PMSK*, S, and the random nonce $n1$ and $n2$. The target gNB-DU then computes the message authentication codes *HM*3 and *HM*4 using *SK* and *PMSK*, respectively. Next, it constructs the Random-Access Response message including R, $n1$, $n2$, *HM*3 and *HM*4. It then transmits this message to the UE.

Step 10: The UE verifies the message authentication code *HM*4 with *PMSK*. If *HM*4 is valid, the UE computes the ECDH session key S using the target gNB-DU's ECDH public key R and its ECDH private key X. The UE also derives the session key *SK* using the ECDH session key S, the pre-wise master key *PMSK*, and random nonce $n1$ and $n2$. Subsequently, it verifies the validity of *HM*3 by using *SK* and the UE generates the message authentication code *HM*5 with *SK* and transmits it with the RRC Connection Reconfiguration Complete message to the target gNB-DU.

Step 11: The target gNB-DU verifies the message authentication code *HM*5 with the session key *SK*. If it is valid, the target gNB-DU sends the Uplink RRC Transfer message to the gNB-CU to inform that the handover procedure is complete.

Step 12: When the gNB-CU receives the Uplink RRC Transfer from the target gNB-DU, the gNB-CU instructs the source gNB-DU to release the allocated resources through the UE Context Release Command message.

Step 13: The source gNB-DU then releases the allocated resources and reports them to the gNB-CU through the UE Context Release Complete message. This message concludes the handover phase of the protocol.

A visual illustration of the inter-gNB-DU handover using the proposed protocol for 5G enabled vehicular communications is shown in Figure 10. The figure expresses the different protocol passes numbered for Init and HO phases of the protocol.

IV. FORMAL VERIFICATION

It is vital to check if the proposed handover security protocol is secure against known attacks and satisfies its security requirements. Consequently, this section formally verifies the security of the protocol (in both the initial phase and handover phase) by using BAN logic [20] and Scyther [21], which are known formal verification tools. The former is a modal logic-based verification mechanism proposed by Burrows, Abadi, and Needham. The latter, presented by Cas Cremers, is an automated tool for formal protocol analysis, verification, and falsification [21].

A. FORMAL VERIFICATION WITH BAN LOGIC

BAN logic follows four procedures, each with its laws and notations: (1) Idealization, (2) Assumption, (3) Goal, and (4) Derivation. The non-plain information such as encrypted messages, digital signatures, and message authentication codes are modeled in Idealization using the rules

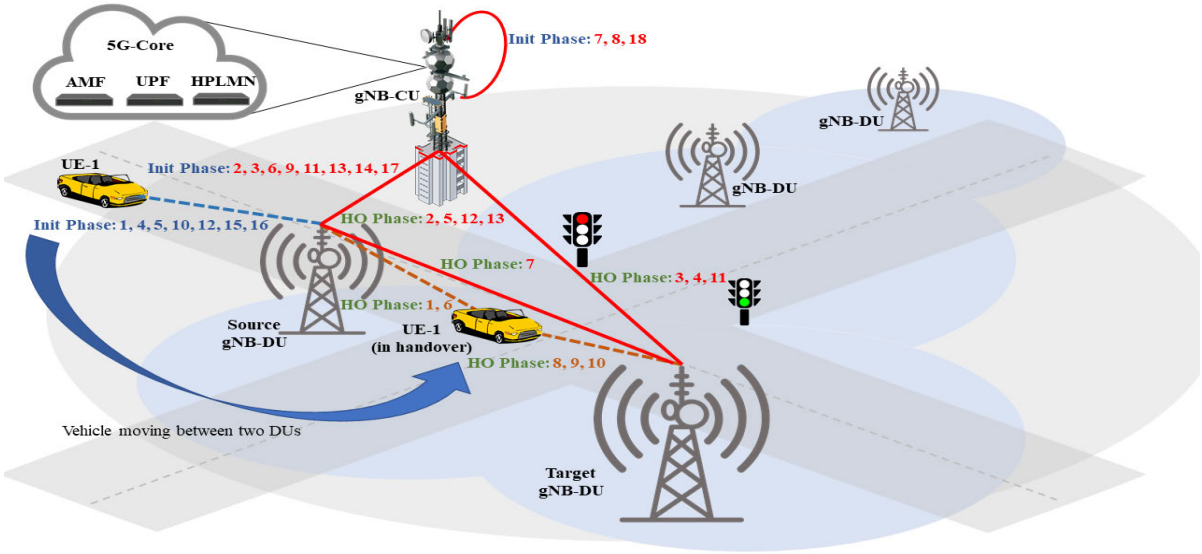


FIGURE 10. An illustration of the inter-gNB-DU handover using the proposed protocol for 5G enabled vehicular communications.

TABLE 3. Notations of BAN logic.

Notation	Description
$P\| \equiv X$	P believes that the message X is true
$P \lhd X$	P receives the message X at any point in time
$P\|\sim X$	P previously sent the message X
$P\| \Rightarrow X$	P has jurisdiction over X
$\#(X)$	X is fresh
$P \overset{K}{\leftrightarrow} Q$	K is a secret key shared between P and Q
$P \overset{K}{\Leftrightarrow} Q$	K is a shared secret between P and Q.
$\{X\}_K$	X is encrypted with a key K
X, Y	X is combined with Y

TABLE 4. Rules of BAN logic.

Rule	Description
Message Meaning Rule (MM)	$\frac{P\| \equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P\| \equiv Q\|\sim X}$ $\frac{P\| \equiv P \overset{K}{\Leftrightarrow} Q, P \lhd \langle X\rangle_K}{P\| \equiv Q\|\sim X}$ $\frac{P\| \equiv \overset{K}{\rightarrow} Q, P \lhd \{X\}_{K^{-1}}}{P\| \equiv Q\|\sim X}$
Nonce Verification Rule (NV)	$\frac{P\| \equiv \#(X), P\| \equiv Q\|\sim X}{P\| \equiv Q\| \equiv X}$
Jurisdiction Rule (JR)	$\frac{P\| \equiv Q\| \Rightarrow X, P\| \equiv Q\| \equiv X}{P\| \equiv X}$
Freshness Rule (FR)	$\frac{P\| \equiv \#(X)}{P\| \equiv \#(X, Y)}$
Decomposition Rule (DR)	$\frac{P \lhd (X, Y)}{P \lhd X}$
Belief Conjunction Rule (BC)	$\frac{P\| \equiv X, P\| \equiv Y}{P\| \equiv (X, Y)}$ $\frac{P\| \equiv Q\| \equiv (X, Y)}{P\| \equiv Q\| \equiv X}$ $\frac{P\| \equiv Q\|\sim (X, Y)}{P\| \equiv Q\|\sim X}$
Diffie-Hellman Rule (DH)	$\frac{P\| \equiv Q\|\sim \overset{Y.G}{\longrightarrow} Q, P\| \equiv \overset{X.G}{\longrightarrow} P}{P\| \equiv P \overset{X.Y.G}{\longleftrightarrow} Q}$

and notations. Following Idealization, suitable Assumptions and Goals are established, and Derivations are carried out using the other three procedures together with the intermediate results of the derivation process. Table 3 and Table 4 demonstrate the BAN logic notations and laws, respectively. Also, in the BAN logic analysis, CU and DU denote gNB-CU and gNB-DU, respectively. The formal verification of the proposed protocol using BAN Logic is performed as follows.

1) INITIAL PHASE

The idealization form of the initial phase of the protocol are shown below:

$$UE \rightarrow CU : \left\langle ID_{UE}, Q, U\ E \overset{K}{\leftrightarrow} CU \right\rangle_K \quad \text{(I1)}$$

$$DU \rightarrow UE : \left\langle ID_{DU}, Q, R, U\ E \overset{MSK}{\longleftrightarrow} DU, U\ E \overset{K}{\leftrightarrow} CU \right\rangle_K \quad \text{(I2)}$$

$$UE \rightarrow DU : \langle UE \overset{MSK}{\longleftrightarrow} DU \rangle_{MSK} \quad \text{(I3)}$$

The realistic assumptions concerning the security keys and their freshness for gNB-CU (A1-A3 and A6),

UE (A4 and A5), and gNB-DU (A7 and A8) are formulated as shown below.

$$CU| \equiv UE \overset{K}{\longleftrightarrow} CU \quad (A1)$$
$$CU| \equiv \#(K) \quad (A2)$$
$$CU| \equiv \overset{R}{\longrightarrow} CU \quad (A3)$$
$$E| \equiv UE \overset{K}{\longleftrightarrow} CU \quad (A4)$$
$$UE| \equiv \#(Q) \quad (A5)$$
$$UE| \equiv \overset{Q}{\longrightarrow} UE \quad (A6)$$
$$DU| \equiv UE \overset{MSK}{\longleftrightarrow} DU \quad (A7)$$
$$DU| \equiv \#(MSK) \quad (A8)$$

The goals to be achieved for verification of the initial phase are defined as follows. Here, (G1) and (G4) illustrate the secure exchange of the identifier of the user equipment (UE) and the network (gNB-DU), while (G2) and (G5) denote security of the pre-shared keys (such as K_{gNB}). The remaining goals demonstrate the successful exchange of the master key *MSK* between the UE and the gNB-DU.

$$CU| \equiv UE| \equiv ID_{UE} \quad (G1)$$
$$CU| \equiv UE| \equiv UE \overset{K}{\longleftrightarrow} CU \quad (G2)$$
$$CU| \equiv UE \overset{MSK}{\longleftrightarrow} DU \quad (G3)$$
$$UE| \equiv DU| \equiv ID_{DU} \quad (G4)$$
$$UE| \equiv DU| \equiv UE \overset{K}{\longleftrightarrow} CU \quad (G5)$$
$$UE| \equiv UE \overset{MSK}{\longleftrightarrow} DU \quad (G6)$$
$$UE| \equiv DU| \equiv UE \overset{MSK}{\longleftrightarrow} DU \quad (G7)$$
$$DU| \equiv UE| \equiv UE \overset{MSK}{\longleftrightarrow} DU \quad (G8)$$

Here, the BAN logic rules are applied to the idealization, the assumptions, and the intermediate outputs to derive the goals.

From (I1):

$$CU \triangleleft \left\langle ID_{UE}, Q, U\ E \overset{K}{\leftrightarrow} CU \right\rangle_K \quad (D1)$$
$$CU| \equiv UE| \sim \left[ID_{UE}, Q, UE \overset{K}{\longleftrightarrow} CU \right] \text{ by}(D1), (A1), MM \quad (D2)$$
$$CU| \equiv UE| \equiv \left[ID_{UE}, Q, UE \overset{K}{\longleftrightarrow} CU \right] \text{ by } (D2), (A2), FR, NV \quad (D3)$$
$$CU| \equiv UE| \equiv ID_{UE} \text{by } (D3), BC \quad (D4)$$
$$CU| \equiv UE| \equiv UE \overset{K}{\longleftrightarrow} CU \text{by } (D3), BC \quad (D5)$$
$$CU| \equiv S \text{by } (D2), (A3), BC, DH \quad (D6)$$
$$CU| \equiv UE \overset{MSK}{\longleftrightarrow} DU \text{by } (D5), (A1), BC \quad (D7)$$

From (I2):

$$UE \triangleleft \left\langle ID_{DU}, Q, R, U\ E\ {}^{MSK} \longleftrightarrow DU, U\ E\ \overset{K}{MSK} \leftrightarrow CU \right\rangle_{K_K} \quad (D8)$$

$$UE| \equiv DU| \sim \left[ID_{DU}, Q, R, UE \overset{MSK}{\longleftrightarrow} DU, UE \overset{K}{\longleftrightarrow} CU \right] \text{ by } (D7), (A4), MM \quad (D9)$$
$$UE| \equiv DU| \equiv \left[ID_{DU}, Q, R, UE \overset{MSK}{\longleftrightarrow} DU, UE \overset{K}{\longleftrightarrow} CU \right] \text{ by } (D8), (A5), FR, NV \quad (D10)$$
$$UE| \equiv DU| \equiv ID_{DU} \text{ by } (D10), BC \quad (D11)$$
$$UE| \equiv DU| \equiv UE \overset{K}{\longleftrightarrow} CU \text{ by } (D10), BC \quad (D12)$$
$$UE| \equiv S \text{by } (D9), (A6), BC, DH \quad (D13)$$
$$UE| \equiv UE \overset{MSK}{\longleftrightarrow} DU \text{ by } (D13), (A4), BC \quad (D14)$$
$$UE| \equiv DU| \equiv UE \overset{MSK}{\longleftrightarrow} DU \text{ by } (D10), BC \quad (D15)$$

From (I3):

$$DU \triangleleft \langle UE \overset{MSK}{\longleftrightarrow} DU \rangle_{MSK} \quad (D16)$$
$$UE| \equiv DU| \sim UE \overset{MSK}{\longleftrightarrow} DU \text{ by } (D16), (A7), MM \quad (D17)$$
$$UE| \equiv DU| \equiv UE \overset{MSK}{\longleftrightarrow} DU \text{ by } (D17), (A8), FR, NV \quad (D18)$$

The above derivations show that all goals have been realized. The following lemmas further illustrate these goals:

Theorem 1: The Initial Phase of the proposed protocol is secure.

Proof of Theorem 1: Through the proofs of Lemma 1-1 to Lemma 1-4, the defined goals are satisfied, and hence, the initial phase of the proposed protocol is secure. □

Lemma 1-1: The Initial Phase of the proposed protocol can provide mutual authentication.

Proof of Lemma 1-1: The derived belief (D4) shows that the gNB-CU authenticates the UE, and (D11) shows the UE authenticates the gNB-DU. In the initial phase, the gNB-CU authenticates the UE on behalf of the gNB-DU. The gNB-CU should authenticate the UE because there is no pre-shared key between them. □

Lemma 1-2: The master key MSK is successfully exchanged between the UE and the gNB-DU.

Proof of Lemma 1-2: The UE can believe the master key *MSK* through the derived beliefs (D14) and (D15). The gNB-DU can indirectly believe the master key *MSK* through (D18). For the direct belief (D7), the gNB-CU generates the master key *MSK* instead of the gNB-DU and transfers it through a secure channel. □

Lemma 1-3: The Initial Phase of the proposed protocol can provide the perfect forward secrecy.

Proof of Lemma 1-3: According to (D6) and (D13), the master key *MSK* is generated with the ECDH session key S. The secure key exchange of this key via ECDHE is ephemeral in the sense that for each session, a new session key is used, which guarantees the perfect forward secrecy of the initial phase of the proposed protocol. □

Lemma 1-4: The Initial Phase of the proposed protocol can provide confidentiality and integrity.

Proof of Lemma 1-4: Based on Lemma 1-2, the UE and the gNB-DU exchange the master key *MSK*. Also, it can prove that the initial phase of the proposed protocol can provide

the perfect forward secrecy through Lemma 1-3. Therefore, the secret key exchanged between the UE and the gNB-DU is secure, and by extension, the initial phase of the proposed protocol provides confidentiality. On the other hand, the UE and the gNB-DU believe the master key *MSK* through (D14) and (A7), and they can also believe that the other believes the master key *MSK* through (D15) and (D18). With these beliefs, the UE and the gNB-DU can believe that the message has not been altered in transit. □

2) HANDOVER PHASE

The idealization forms of the handover phase are shown below. In the BAN logic formulas, the source and target gNB-DUs are denoted as source gNB-DU (sDU) and target gNB-DU (tDU), respectively.

$$UE \rightarrow tDU : \left\langle ID_{UE}, Q, n_1, U\ E \overset{PMSK}{\longleftrightarrow} CU \right\rangle_{PMSK} \quad \text{(I4)}$$

$$tDU \rightarrow UE : \left\langle ID_{tDU}, R, n_1, n_2, U\ E \overset{SK}{\leftrightarrow} tDU, U\ E \overset{PMSK}{\longleftrightarrow} tDU \right\rangle_{PMSK} \quad \text{(I5)}$$

$$UE \rightarrow tDU : \left\langle n_2, U\ E \overset{SK}{\leftrightarrow} tDU \right\rangle_{SK} \quad \text{(I6)}$$

The assumptions made in this phase of the protocol are basically about the pre-wise master key *PMSK* (that is distributed to the target gNB-DU by the gNB-CU) (A9-A10 and A12), the ECDH public keys Q and R (A11 and A14), and freshly generated nonces $n1$ and $n2$ (A13 and A15).

$$tDU| \equiv UE \overset{PMSK}{\longleftrightarrow} tDU \quad \text{(A9)}$$
$$tDU| \equiv \#(PMSK) \quad \text{(A10)}$$
$$tDU| \equiv \overset{R}{\longrightarrow} tDU \quad \text{(A11)}$$
$$UE| \equiv UE \overset{PMSK}{\longleftrightarrow} tDU \quad \text{(A12)}$$
$$UE| \equiv \#(n_1) \quad \text{(A13)}$$
$$UE| \equiv \overset{Q}{\longrightarrow} UE \quad \text{(A14)}$$
$$tDU| \equiv \#(n_2) \quad \text{(A15)}$$

The final goals of the Handover Phase for the target gNB-DU (G9 – G11 and G16) and UE (G12 –G15) are defined as shown below.

$$tDU| \equiv UE| \equiv ID_{UE} \quad \text{(G9)}$$
$$tDU| \equiv UE| \equiv UE \overset{PMSK}{\longleftrightarrow} tDU \quad \text{(G10)}$$
$$tDU| \equiv UE \overset{SK}{\longleftrightarrow} DU \quad \text{(G11)}$$
$$UE| \equiv tDU| \equiv ID_{tDU} \quad \text{(G12)}$$
$$UE| \equiv tDU| \equiv UE \overset{PMSK}{\longleftrightarrow} CU \quad \text{(G13)}$$
$$UE| \equiv tDU| \equiv UE \overset{SK}{\longleftrightarrow} CU \quad \text{(G14)}$$
$$UE| \equiv UE \overset{SK}{\longleftrightarrow} DU \quad \text{(G15)}$$
$$tDU| \equiv UE| \equiv UE \overset{SK}{\longleftrightarrow} DU \quad \text{(G16)}$$

The eight goals set for tDU and UE above are derived as shown below.

From (I4):

$$tDU \triangleleft \left\langle ID_{UE}, Q, U\ E \overset{PMSK}{\longleftrightarrow} tDU \right\rangle_{PMSK} \quad \text{(D19)}$$
$$tDU| \equiv UE| \sim \left[ID_{UE}, Q, UE \overset{PMSK}{\longleftrightarrow} tDU \right] by\,(D19)\,,(A9)\,,MM \quad \text{(D20)}$$
$$tDU| \equiv UE| \equiv \left[ID_{UE}, Q, UE \overset{PMSK}{\longleftrightarrow} tDU \right] by\,(D20)\,,(A10)\,,FR,NV \quad \text{(D21)}$$
$$tDU| \equiv UE| \equiv ID_{UE} by\,(D21)\,,BC \quad \text{(D22)}$$
$$tDU| \equiv UE| \equiv UE \overset{PMSK}{\longleftrightarrow} CU by\,(D21)\,,BC \quad \text{(D23)}$$
$$tDU| \equiv Sby\,(D20)\,,(A11)\,,BC,DH \quad \text{(D24)}$$
$$tDU| \equiv UE \overset{SK}{\longleftrightarrow} DU by\,(D24)\,,(A9)\,,BC \quad \text{(D25)}$$

From (I5):

$$UE \propto \left\langle ID_{tDU}, R, U\ E \overset{MSK}{\longleftrightarrow} tDU, U\ E \overset{PMSK}{\longleftrightarrow} tDU \right\rangle_{PMSK} \quad \text{(D26)}$$
$$UE| \equiv tDU| \sim \left[ID_{tDU}, R, UE \overset{SK}{\longleftrightarrow} tDU, UE \overset{PMSK}{\longleftrightarrow} tDU \right] by\,(D26)\,,(A12)\,,MM \quad \text{(D27)}$$
$$UE| \equiv tDU| \equiv \left[ID_{tDU}, R, UE \overset{SK}{\longleftrightarrow} tDU, UE \overset{PMSK}{\longleftrightarrow} tDU \right] by\,(D27)\,,(A13)\,,FR,NV \quad \text{(D28)}$$
$$UE| \equiv tDU| \equiv ID_{tDU} by\,(D28)\,,BC \quad \text{(D29)}$$
$$UE| \equiv tDU| \equiv UE \overset{PMSK}{\longleftrightarrow} tDU by\,(D28)\,,BC \quad \text{(D30)}$$
$$UE| \equiv tDU| \equiv UE \overset{SK}{\longleftrightarrow} tDU by\,(D28)\,,BC \quad \text{(D31)}$$
$$UE| \equiv Sby\,(D27)\,,(A14)\,,BC,DH \quad \text{(D32)}$$
$$UE| \equiv UE \overset{SK}{\longleftrightarrow} tDU by\,(D32)\,,(A12)\,,BC \quad \text{(D33)}$$

From (I6):

$$DU \triangleleft \langle UE \overset{MSK}{\longleftrightarrow} DU \rangle_{MSK} \quad \text{(D34)}$$
$$UE| \equiv DU| \sim \left[UE \overset{MSK}{\longleftrightarrow} DU \right] by\,(D16)\,,(A7)\,,MM \quad \text{(D35)}$$
$$UE| \equiv DU| \equiv UE \overset{MSK}{\longleftrightarrow} DU by\,(D17)\,,(A8)\,,FR,NV \quad \text{(D36)}$$

According to the above derivations (D19)-(D36), the goals (G9)-(G16) are achieved. Next, we show that the security requirements are satisfied by using Theorem 2 and the following Lemmas.

Theorem 2: The Handover Phase of the proposed protocol is secure.

Proof of Theorem 2: Through Lemma 2-1 to Lemma 2-4, the defined goals are satisfied that the handover phase of the proposed protocol is secure. □

Lemma 2-1: The Handover Phase of the proposed protocol can provide mutual authentication.

Proof of Lemma 2-1: The derivations (D22) and (D29) show that the target gNB-DU and the UE have mutually authenticated each other. □

Lemma 2-2: The pre-wise master key MSK and the session key SK are successfully exchanged between the UE and the target gNB-DU (tDU).

Proof of Lemma 2-2: The UE and the target gNB-DU have a direct belief in the pre-master key *PMSK* through the assumptions (A9) and (A12). Also, the direct belief in the session key *SK* can be supported by the derivations (D25) and (D33). On the other hand, the indirect belief of the UE and the target gNB-DU to the pre-wise master key *PMSK* can be proved with (D23) and (D30) and in the session key *SK* with (D31) and (D36). □

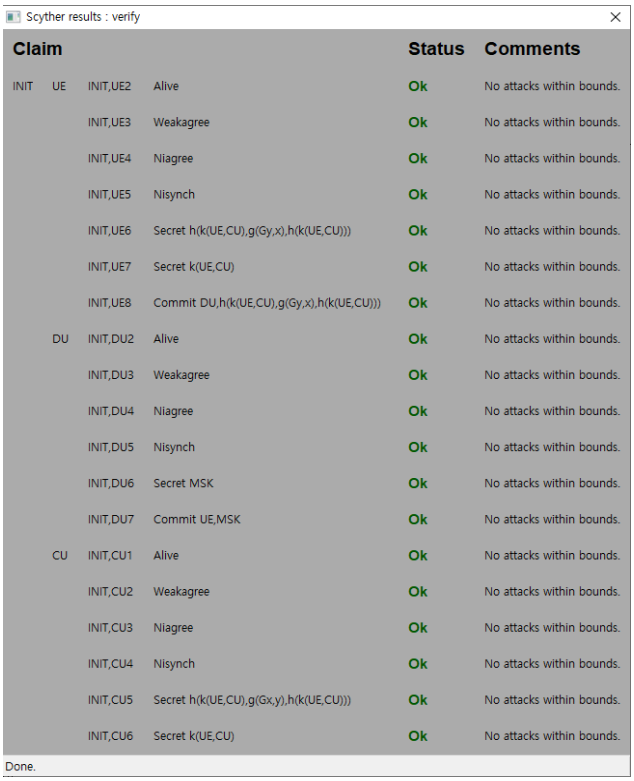
Lemma 2-3: The Handover Phase of the proposed protocol can provide the perfect forward secrecy.

Proof of Lemma 2-3: Like Lemma 1-3, the session key *SK* is generated from the non-static ECDH session key *S* between UE and tDU in (D25) and (D33). Therefore, the handover phase of the proposed protocol can support the perfect forward secrecy. □

Lemma 2-4: The Handover Phase of the proposed protocol can provide confidentiality and integrity.

Proof of Lemma 2-4: From above Lemma 2-2 and Lemma 2-3, the session key *SK* is successfully exchanged between the UE and the target gNB-DU. Consequently, it can be shown that the handover phase of the proposed protocol can provide confidentiality and integrity via the session key *SK*. □

In conclusion, Theorem 1 and Theorem 2 prove that both phases of the proposed protocols are secure. In other words, the above Theorems and Lemmas show that the security requirements of the proposed protocol are satisfied.


Scyther results : verify

Claim				Status	Comments
INIT	UE	INIT,UE2	Alive	Ok	No attacks within bounds.
		INIT,UE3	Weakagree	Ok	No attacks within bounds.
		INIT,UE4	Niagree	Ok	No attacks within bounds.
		INIT,UE5	Nisynch	Ok	No attacks within bounds.
		INIT,UE6	Secret h(k(UE,CU),g(Gy,x),h(k(UE,CU)))	Ok	No attacks within bounds.
		INIT,UE7	Secret k(UE,CU)	Ok	No attacks within bounds.
		INIT,UE8	Commit DU,h(k(UE,CU),g(Gy,x),h(k(UE,CU)))	Ok	No attacks within bounds.
	DU	INIT,DU2	Alive	Ok	No attacks within bounds.
		INIT,DU3	Weakagree	Ok	No attacks within bounds.
		INIT,DU4	Niagree	Ok	No attacks within bounds.
		INIT,DU5	Nisynch	Ok	No attacks within bounds.
		INIT,DU6	Secret MSK	Ok	No attacks within bounds.
		INIT,DU7	Commit UE,MSK	Ok	No attacks within bounds.
	CU	INIT,CU1	Alive	Ok	No attacks within bounds.
		INIT,CU2	Weakagree	Ok	No attacks within bounds.
		INIT,CU3	Niagree	Ok	No attacks within bounds.
		INIT,CU4	Nisynch	Ok	No attacks within bounds.
		INIT,CU5	Secret h(k(UE,CU),g(Gx,y),h(k(UE,CU)))	Ok	No attacks within bounds.
		INIT,CU6	Secret k(UE,CU)	Ok	No attacks within bounds.

Done.

FIGURE 11. Verification result with scyther (initial phase).

B. FORMAL VERIFICATION WITH SCYTHER

BAN-Logic has an essential role in analyzing authentication protocols by leveraging modal logics of beliefs to express authentication protocols while revealing redundancies succinctly. However, it has some limitations, including inaccurate message representations in the Idealization step [22] and inference rules associated with hash functions [23]. As a result, utilizing automated formal verification, falsification, and analysis tools, such as Scyther [24], can assist overcome these constraints and boost the confidence of the verification outcome. Hence, it is preferable to use more than one verification technique to compensate for the shortcomings of the others.

In this section, we use Scyther to model the target protocol based on SPDL (Security Protocol Language Description) and checks its security through claim events. Scyther automatically searches for possible attacks if the target protocol is insecure. In other words, Scyther analyzes SPDL to verify if the modeled protocol violates the claim events (i.e., 'Alive', 'Nisynch', 'Niagree', 'Weakagree', 'Running/Commit, and Secret [24]).

The verification process starts by modeling the initial and handover phases of the protocol through SPDL with different claim events. Here, while the initial phase's SPDL includes the UE's role (UE), the gNB-DU's role (DU), and gNB-CU's role (CU), the handover phase adds the source and target gNB-DUs. Each role communicates with the other through the channel set 'send' and 'recv'.

Figures 11 and 12 show that Scyther checks whether the proposed protocol can provide authentication and secrecy. If the proposed protocol satisfied the requirements, the result displays all the event claims labeled 'OK'. If not, it shows how the attack happens. Consequently, the verification results from Scyther show that the proposed protocol is secure against known attacks.

V. COMPARISON ANALYSIS

To the best of our knowledge, this paper pioneers designing a security protocol for the inter-gNB-DU handover scenarios. Despite that, we believe that it is possible to use the different variants of the EAP protocols that are widely used in mobile communication (EAP-AKA' [17], EAP-AKA [25], EAP-TLS [26], and EAP-IKEv2 [27]) to cover the security between UE and gNB-DU. For comparison purposes, this section analyses the computational overhead (Table 5), security requirement satisfaction (Table 6), and handover communication cost (Figure 13) of our proposed protocol and EAP protocols.

According to Table 5, the suggested protocol outperforms [26] and [27] in terms of computing overhead since it does not require a certificate (C_6) and asymmetric encryption operations (C_2). On the contrary, [17] and [25] have less computing overhead than the proposed protocol. However, as presented in Table 6, both protocols do not support security properties such as perfect forward secrecy and optimized handover.

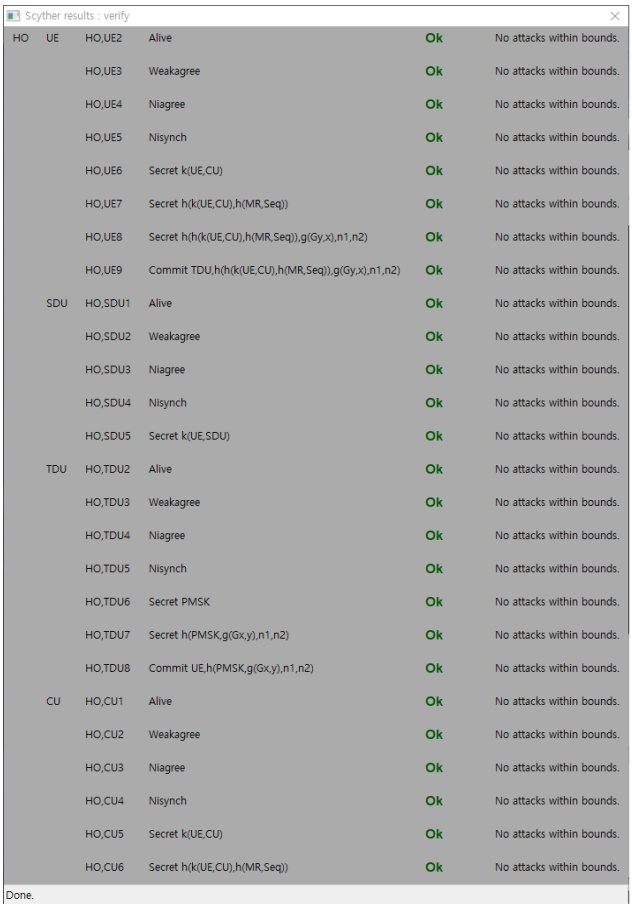


FIGURE 12. Verification result with scyther (handover phase).

TABLE 5. Comparison in terms of computational overhead with existing works.

Protocols	Computational Overheads			
	UE	sDU	tDU	CU/AAA
[17]	$9C_5$	-	$1C_5$	$8C_5$
[25]	$9C_5$	-	-	$9C_5$
[26]	$1C_1+1C_2+4C_5+1C_6$	-	$1C_2+1C_1+1C_3+1C_4+1C_5$	-
[27]	$3C_1+1C_3+1C_4+1C_5+1C_6+1C_7$	-	$3C_1+1C_3+1C_4+1C_5+1C_6+1C_7$	-
Proposed protocol (Init)	$4C_5+1C_7$	$1C_5$	-	$3C_5+1C_7$
Proposed protocol (HO)	$7C_5+1C_7$	$1C_5$	$5C_5+1C_7$	$1C_5$

C_1: Symmetric encryption/decryption overhead;
C_2: Asymmetric encryption/decryption overhead;
C_3: Digital signature overhead;
C_4: Signature validation overhead;
C_5: One-way HMAC overhead;
C_6: Certificate validation overhead;
C_7: ECDH operational overhead

In line with the comparison results shown in Table 6, all four protocols support confidentiality, integrity, mutual authentication, and key exchange. However, [17], [25], and [26] fail to support perfect forward secrecy and optimized handover, and [27] does not support the latter one. In conclusion, only the proposed protocol can satisfy all the security properties.

TABLE 6. Comparison in terms of security properties with existing works.

Security Property	[8]	[17]	[25]	[26]	[27]	Proposed Protocol
SP1	X	O	O	O	O	O
SP2	X	O	O	O	O	O
SP3	X	O	O	O	O	O
SP4	X	O	O	O	O	O
SP5	X	X	X	X	O	O
SP6	X	X	X	X	X	O

SP1: Confidentiality; SP2: Integrity; SP3: Mutual authentication; SP4: Key exchange; SP5: Perfect forward secrecy; SP6: Optimized handover; O: Support; X: Not support

The comparison results from Table 5 and Table 6 show that the proposed protocol provides efficient and secure communications between the UE and the gNB-DUs.

Moreover, the optimized handover among the gNB-DUs eliminated inefficient parts such as repetitive operations during handover. It is worth noting that the overhead in CU is eliminated (despite the challenging nature of resolving the traffic concentration between the UE and the gNB) by distributing traffics to the gNB-DUs.

To further demonstrate the advantage of the proposed protocol, we compare its handover communication cost (HCC) against those EAP protocols. The HCC refers to the total execution time of signaling messages to complete the transfer of UE's point of attachment to a target DU while achieving mutual authentication. Accordingly, we express the communication cost during the handover scenario of our proposed protocol as follows:

$$L_{PRO} = T_{<UE-sDU>} + 5 * T_{<sDU-CU>} + 3 * T_{<tDU-CU>} + DU_{L2} + \delta$$

among which $T_{<entities>}$ is the transmission delay between the involved entities, δ is the time to finish connection resumption encompassing random access procedure and connection reconfiguration messages, and DU_{L2} refers to layer 2 and RLC layer processing latency of each message received by the DUs. In addition, assuming that the DU and CU entities are in different locations with a wired connection (e.g., optic-fiber), the transmission delay is given as $T_{<*DU-CU>} = d * \zeta$ where d is the radial distance of DUs to CU, and δ is the average transmission delay per kilometer.

Meanwhile, the EAP protocols used for comparison can be candidates for authentication between the UE and DU when the former transfers its point of attachment. In this case, the full-authentication procedure of these considered protocols is executed, i.e., the UE, target DU, and CU adopt

the peer, authenticator, and authentication server role in EAP protocols, respectively. Accordingly, the latency of EAP-AKA' ($L_{AKA'}$), EAP-AKA (L_{AKA}), EAP-TLS (L_{TLS}), and EAP-IKEv2 (L_{IKEv2}) is given as follows:

$$\begin{aligned} L_{AKA'} = L_{AKA} &= 4 * T_{<UE-tDU>} + 3 * T_{<tDU-CU>} \\ &+2 * UE_{L2} + 2 * DU_{L2} \\ &+2 * T_{<sDU-CU>} + \delta \\ L_{TLS} &= 8 * T_{<UE-tDU>} + 9 * T_{<tDU-CU>} + 4 * UE_{L2} \\ &+4 * DU_{L2} + 2 * T_{<sDU-CU>} + \delta \\ L_{IKEv2} &= 6 * T_{<UE-tDU>} + 7 * T_{<tDU-CU>} + 3 * UE_{L2} \\ &+3 * DU_{L2} + 2 * T_{<sDU-CU>} + \delta \end{aligned}$$

Here, UE_{L2} denotes the processing latency of layer 2 and RLC layer at the UE.

To follow the handover communication cost, we used numerical simulations parameters from [28] and [29] for the evaluation, as summarized in Table 7.

TABLE 7. Numerical parameters [28], [29].

Parameters	Values
$T_{<UE-xDU>}$	1 ms
d	20 – 100 km
ζ	0.05 ms/km
δ	9.5 ms
UE_{L2}	5 ms
DU_{L2}	4/3 ms

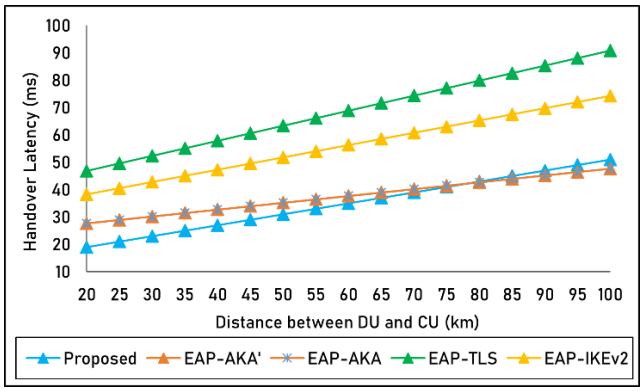


FIGURE 13. Total communication cost vs DU-CU radial distance.

Figure 13 shows the handover communication cost of EAP protocols and our proposed extended intra-DU handover. As illustrated in this figure, the costs of the EAP protocols are generally higher than our proposed protocol since their corresponding full-authentication procedure is executed. The TLS protocol incurs the highest communication cost among the EAP protocols due to the higher signaling overhead. We can also observe that the EAP-AKA and EAP-AKA' incur equal costs because they contain the same number of signaling message sequences. However, it is essential to note that the radial distance between CU and DU is significant since it affects the communication cost of our proposed protocol. Apparently, EAP-AKA and EAP-AKA' provide better results than the proposed protocol when the radial distance is above 80 kilometers. These results are due to the relatively higher number of signaling messages between CU and DUs. Nevertheless, [28] suggests that a remotely located DU has a radial distance between 20 to 40 kilometers from CU. Within such range, our proposed protocol incurs the smallest communication cost.

VI. CONCLUSION

The 5G mobile network infrastructure, composing small-cell base stations, will serve as the vital foundation for V2X services. The small-coverage nature of these base stations, along with the functional split architecture of NG-RAN into gNB-CU and multiple gNB-DU, inevitably causes more frequent handover scenarios of UE between the latter, especially to fast-moving devices such as vehicles. However, the current 5G standard does not support secure channel configuration at the gNB-DU level, making the inter-gNB-DU handover signaling messages exposed to a range of security threats, such as resource depletion, denial of service, association to a false base station, and many more. Such security concern is grave, especially to the safety-critical V2X applications; hence, security measures are imperative to alleviate the problem. Accordingly, this paper proposes an inter-gNB-DU handover security protocol for vehicular networks, satisfying essential security requirements including confidentiality, integrity, mutual authentication, secure key exchange, and perfect forward secrecy. In the first phase of the protocol, called the initial phase, the UE and the serving gNB-DU (via gNB-CU) computes mutual authentication and agree on a master key MSK. In the second phase, called the handover phase, UE is securely handed over to a target gNB-DU using the shared MSK and other derived keys. To examine the proposed protocol's capability to withstand attacks and fulfill standard security properties, we have performed formal security verification using BAN logic and Scyther. The verification results show that both phases of the protocol are safe and satisfy the security requirements set.

Furthermore, we compared the proposed protocol against well-known security protocols (EAP-AKA', EAP-AKA, EAP-TLS, and EAP-IKEv2) concerning security property and computational and communication overheads. Overall, the proposed protocol offers a secure and optimized handover scheme while showing strong security and low overheads compared to the existing protocols. It is worth mentioning that the suggested protocol is mainly efficient for "after-handover-decision" processes. However, it is possible to improve this by determining the handover target by predicting the UE's movement. This way, it is possible to reduce the wasted resources for the handover. As future work, we plan to incorporate such an optimization technique for efficient resource allocation during the inter-gNB-DU

situation. In addition, we will also further investigate the identified vulnerabilities and validate them using open-source simulation tools, like UERANSIM [30].

REFERENCES

[1] V. Sharma, J. Kim, Y. Ko, I. You, and J. T. Seo, "An optimal security management framework for backhaul-aware 5G-vehicle to everything (V2X)," *J. Internet Technol.*, vol. 21, no. 1, pp. 245–260, Jan. 2020.

[2] M. Kang, "The study on the effect of the internet and mobile-cellular on trade in services: Using the modified gravity model," *J. Internet Services Inf. Secur.*, vol. 10, no. 4, pp. 90–100, Nov. 2020.

[3] *Study on 5G Security Enhancements Against False Base Stations (FBS) (Release 17)*, document 3GPP TS 33.809, Version 0.13.0, 3GPP, Jan. 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539

[4] P. S. L. M. Barreto, M. A. Simplicio, J. E. Ricardini, and H. K. Patil, "Schnorr-based implicit certification: Improving the security and efficiency of vehicular communications," *IEEE Trans. Comput.*, vol. 70, no. 3, pp. 393–399, Mar. 2021.

[5] S. Chen, J. Hu, Y. Shi, L. Zhao, and W. Li, "A vision of C-V2X: Technologies, field testing, and challenges with Chinese development," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3872–3881, May 2020.

[6] V. Sharma, I. You, and N. Guizani, "Security of 5G-V2X: Technologies, standardization, and research directions," *IEEE Netw.*, vol. 34, no. 5, pp. 306–314, Sep. 2020.

[7] S. K. Tayyaba, H. A. Khattak, A. Almogren, M. A. Shah, I. U. Din, I. Alkhalifa, and M. Guizani, "5G vehicular network resource management for improving radio access through machine learning," *IEEE Access*, vol. 8, pp. 6792–6800, Jan. 2020.

[8] *NG-RAN; Architecture Description (Release 16)*, document 3GPP TS 38.401, Version 16.4.0, 3GPP, Jan. 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3219

[9] RCR Wireless News. (2020). *Open RAN 101–RU, DU, CU: Why, What, How, When?* Accessed: Jul. 1, 2021. [Online]. Available: https://www.rcrwireless.com/20200708/open_ran/open-ran-101-ru-du-cu-reader-forum

[10] S. Nowaczewski and W. Mazurczyk, "Securing future internet and 5G using customer edge switching using DNSCrypt and DNSSEC," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 11, no. 3, pp. 87–106, Sep. 2020.

[11] S. K. Wong and S. M. Yiu, "Location spoofing attack detection with pre-installed sensors in mobile devices," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 11, no. 4, pp. 16–30, Dec. 2020.

[12] J. Kim, P. V. Astillo, and I. You, "DMM-SEP: Secure and efficient protocol for distributed mobility management based on 5G networks," *IEEE Access*, vol. 8, pp. 76028–76042, Apr. 2020.

[13] M. A. Ferrag, L. Maglars, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2018.

[14] B. Bertenyi, R. Burbidge, G. Masini, S. Sirotkin, and Y. Gao, "NG radio access network (NG-RAN)," *J. ICT Standardization*, vol. 6, no. 1, pp. 59–76, May 2018.

[15] H. Kim, "5G core network security issues and attack classification from network protocol perspective," *J. Internet Services Inf. Secur.*, vol. 10, no. 2, pp. 1–15, May 2020.

[16] *Security Architecture and Procedure for 5G Systems*, document TS 33.501, Version 17.1.0, 3GPP, Apr. 2021.

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

[18] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 62–67, Feb. 2004.

[19] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[20] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989. Accessed: May 11, 2021. [Online]. Available: https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1989.0125

[21] C. J. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in *Proc. 20th Int. Conf. Comput. Aided Verification (CAV)*, in Lecture Notes in Computer Science, vol. 5123. Princeton, NJ, USA: Springer, Jul. 2008, pp. 414–418.

[22] C. Boyd and W. Mao, "On a limitation of BAN logic," in *Proc. Workshop Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, in Lecture Notes in Computer Science, vol. 765. Berlin, Germany: Springer, May 1993, pp. 240–247.

[23] W. Teepe, "On BAN logic and hash functions or: How an unjustified inference rule causes problems," *Auton. Agents Multi-Agent Syst.*, vol. 19, no. 1, pp. 76–88, Aug. 2009.

[24] C. J. Cremers and S. Mauw, *Operational Semantics and Verification of Security Protocols*. Berlin, Germany: Springer, 2012.

[25] J. Arkko and H. Haverinen, *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*, document IETF RFC 4187, Jan. 2006.

[26] D. Simon, B. Aboba, and R. Hurst, *The EAP-TLS Authentication Protocol*, document IETF RFC 5216, 2008.

[27] H. Tschofenig, D. Kroeselberg, A. Pashalidis, Y. Ohba, and F. Bersani, *The Extensible Authentication Protocol-Internet Key Exchange Protocol Version 2 (EAP-IKEv2) Method*, document IETF RFC 5106, 2008.

[28] G. Brown, "New transport network architecture for 5G RAN," Fujitsu, Kanagawa, Japan, White Paper, 2018. [Online]. Available: https://networking.report/Resources/Whitepapers/34e518ed-c067-4579-adf1-38441f13bc66_New-Transport-Network-Architectures-for-5G-RAN.pdf

[29] Samsung. (Jun. 2017). *4G-5G Interworking: RAN-Level CN-Level Interworking*. [Online]. Available: https://images.samsung.com/is/content/samsung/p5/global/business/networks/insights/white-paper/4g-5g-interworking/global-networks-insight-4g-5g-interworking-0.pdf

[30] A. Güngür. (Jul. 2021). *UERANSIM Release of V3.2.2*. [Online]. Available: https://github.com/aligungr/UERANSIM

JIYOON KIM (Student Member, IEEE) received the M.S. degree in information security engineering from Soonchunhyang University, Asan, South Korea, in 2019, where he is currently pursuing the Ph.D. degree in information security engineering. His current research interests include mobile internet security, 5G security, and formal security analysis.

DANIEL GERBI DUGUMA received the M.Sc. degree in information security engineering from Soonchunhyang University, South Korea, in 2021, where he is currently pursuing the Ph.D. degree with the Department of Information Security Engineering. Prior to this, he worked on financial software and data center projects at Commercial Bank of Ethiopia. His research interests include 5G and beyond security, the medical IoT device security, and formal security analysis.

PHILIP VIRGIL ASTILLO received the B.S. and M.Eng. degrees in computer engineering from the University of San Carlos, Cebu, Philippines, in 2009 and 2011, respectively. He is currently pursuing the Ph.D. degree in information security engineering with Soonchunhyang University, South Korea. From 2009 to 2015, he worked as a Lecturer with the University of San Carlos, where he was a Research Assistant with the Phil-LiDAR Program, from 2014 to 2015. From 2015 to 2016, he was a Research Assistant with the Sensor Laboratory, Clemson University, South Carolina, USA. His research interests include sensor development, embedded system design and development, mobile internet security, 5G security, the IoT application and security, and intrusion detection systems.

HOON-YONG PARK received the B.S. degree in information security engineering from Soonchunhyang University, Asan-si, South Korea, in 2019, where he is currently pursuing the integrated Ph.D. degree with the Department of Information Security Engineering. His research interests include formal security verification and 5G networks.

BONAM KIM received the Ph.D. degree from the Department of Computer Science and Software Engineering, Auburn University, USA, in 2006. She is currently a Research Professor with the Department of Information Security Engineering, Soonchunhyang University, South Korea. Her main research interests include wireless sensor networks, the IoT security, and 5G/6G security.

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 Information Security Engineering, Soonchunhyang University, South Korea. His main 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*, *Intelligent Automation and Soft Computing*.

VISHAL SHARMA (Senior Member, IEEE) received the B.Tech. degree in computer science and engineering from Thapar University, India, in 2012, and the Ph.D. degree in computer science and engineering from Punjab Technical University, in 2016. He is currently working as a Lecturer (an Assistant Professor) with the School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast (QUB), Northern Ireland, U.K. Before coming to QUB, he was a Research Fellow with the Information Systems Technology and Design (ISTD) Pillar, Singapore University of Technology and Design (SUTD), Singapore, where he worked on the future-proof blockchain systems funded by SUTD-MoE. From November 2016 to March 2019, he worked with the Information Security Engineering Department, Soonchunhyang University, South Korea, in multiple positions (from November 2016 to December 2017: a Postdoctoral Researcher and January 2018 to March 2019: a Research Assistant Professor). He held a joint postdoctoral position with Soongsil University, South Korea. He was affiliated with the Industry Academic Cooperation Foundation and the Mobile Internet Security Laboratory, Soonchunhyang University. Before this, he worked as a Lecturer with the Computer Science and Engineering Department, Thapar University. He has authored/coauthored more than 100 journal/conference articles and book chapters and co-edited two books with Springer. His research interests include 5G networks, autonomous systems, aerial (UAV) communications, CPS-IoT behavior-modeling, and mobile internet systems. He was a PC Member and a Reviewer of MIST'16 and MIST'17, respectively. He has served as the TPC Member for ETIC-2019, WiMO-2019, ITNAC-IEEE TCBD'17, ICCMIT'18, CoCoNet'18, and ITNAC-IEEE TCBD'18. He is a Professional Member of ACM and the Past Chair for ACM Student Chapter-TIET Patiala. He was a recipient of three best paper awards from the International Conference on Communication, Management and Information Technology (ICCMIT), Warsaw, Poland, in April 2017; CISC-S'17, South Korea, in June 2017; and IoTaas, Taiwan, in September 2017. He was the Track Chair of MobiSec'16 and AIMS-FSS'16. Furthermore, he serves as a reviewer for various ACM/IEEE TRANSACTIONS and other journals. He serves as an Associate Editor for the *IEEE Communications Magazine*, *CAAI TRIT* (IET), *Wireless Communications and Mobile Computing*, and *IET Networks*. He is serving as a Guest Editor for *MIS*, *IJDSN*, *WCMC*, *Sensors*, *Drones*, *Future Internet* (MDPI), and *Autosoft Journal*.