IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received February 29, 2020, accepted March 13, 2020, date of publication April 3, 2020, date of current version May 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2985448

DMM-SEP: Secure and Efficient Protocol for Distributed Mobility Management Based on 5G Networks

JIYOON KIM, PHILIP VIRGIL ASTILLO, AND ILSUN YOU, (Senior Member, IEEE)
Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea

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

This work was supported in part by The Cross-Ministry Giga Korea Project Funded by the Korea Government (MSIT) under Grant GK19N0600, in part by the Development of 20Gbps Point-To-Multipoint Communication (P2MP) Wireless Backhaul for 5G Convergence Service, and in part by the Soonchunhyang University Research Fund.

ABSTRACT In the 5G era, network mobility management is recognized as a very important factor for user service availability. Especially, due to fast speed and shrinking cell coverage, frequent handover is expected than before. Hence, efficient handover procedure is essential to guarantee seamless service to users. Distributed IP Mobility Management (DMM), a major mobility management solution, is a flat architecture that achieves efficiency and fault tolerance by excluding a centralized anchor and minimizing the distance between a mobile device and its serving network. However, DMM, which has no dominant security scheme specified to itself, is excessively dependent on the security of Layer 2 and is vulnerable to various threats. Especially, the existing security schemes are still venerable to redirection attacks launched by malicious Mobile Access Gateways (MAGs) or Control Mobility Database (CMD). Motivated by this, we proposed a DMM-based handover security protocol that can support privacy and defend against redirection attacks in addition to providing essential security properties such as confidentiality, integrity, mutual authentication, and key exchange. The proposed protocol was formally verified to be correct through AVISPA and BAN logic. Moreover, the comparison analysis showed that the proposed protocol is better than the previous studies and standards.

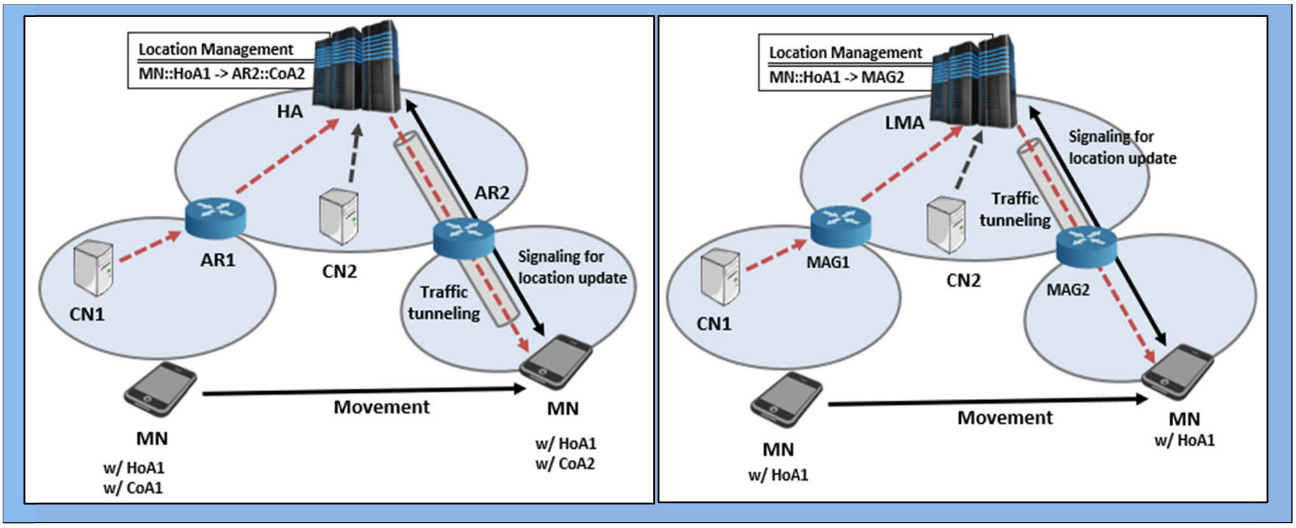
INDEX TERMS Distributed mobility management (DMM), 5G networks, handover security, formal verification.

I. INTRODUCTION

The pervasion of fifth generation (5G) wireless communication technologies is inevitable in the next 4 to 6 years. The design of 5G architecture is expected to leverage heterogeneous network [1] coupled with ultra-dense wireless network [2] to provide a close to ‘‘zero’’ communication latency along with consistent reliability. In such wireless network ecosystem, mobility management (MM) is critical as it should guarantee a sustainable provision of cellular network services while a mobile equipment moves from one service coverage to another. Its main functions include location management and route management. The former focuses on authentication of a user equipment (UE) as well as location tracking as to which access point the UE is connected, whereas the latter manages network route reconfiguration when the UE changes point of attachment. Thus, an effective mobility management protocol should be able to efficiently deliver various network services even though users move at a high rate and their handover events frequently occur, which is expected in 5G network.

Various IP-based mobility management standards have been introduced and they are classified into two categories: host-based and network-based mobility management schemes. First, the host-based mobility management scheme that includes Mobile Internet Protocol version 6 (MIPv6) [3] and its enhanced versions such as Fast Handover MIPv6 (F-MIPv6) [4], Hierarchical MIPv6 (HMIPv6) [5], and Fast Handover for HMIPv6 (F-HMIPv6) [6] requires a mobile node (MN) to be actively involved in the mobility-related signaling process. This approach was not successful as it needs to modify and upgrade MN’s network protocol stack, hence increasing cost and complexity as well as hindering to support legacy devices. Additionally, operators cannot fully

The associate editor coordinating the review of this manuscript and approving it for publication was Antonio Skarmeta Gómez.



(a) *MIPv6* (b) *PMIPv6*

FIGURE 1. Mobility management in CMM; (a) MIPv6 where HA handles mobility functions and routing; (b) PMIPv6 where LMA handles mobility functions and routing.

control a MN's point of attachment because it handles its own mobility service [7]. On the other hand, the network-based approach such as Proxy Mobile Internet Protocol version 6 (PMIPv6) [8] and Fast Handover PMIPv6 (FPMIPv6) [9] was developed and standardized in order to address the weakness of the host-based one. That is, it does not require participation from a MN for managing IIP mobility. All mobility-related signaling are handled by the mobility entities in the network. It is also worth noting that this approach reduces the handoff latency of MNs [10].

The MIPv6 and PMIPv6 schemes are currently the representation of a centralized mobility management protocol (CMM) as show in Figure 1. They are dependent to a certain degree on a centralized mobility anchor, such as Home Agent (HA) and Local Mobility Anchor (LMA), to handle not only the mobility control but also routing of data from a MN to its corresponding node (CN) and vice-versa. In other words, all data traffic goes to the centralized agent (HA and LMA), which then forwards the data to the destination node. The dependency of current mobility solutions to a centralized node are faced with several problems and limitations as enumerated in [11]. The major issues have triggered the Network Working Group of the Internet Engineering Task Force (IETF) to develop and invest effort to standardize a mobility solution that is distributed in nature, now known as Distributed Mobility Management protocol (DMM) [12]. The main concept of the DMM solution to move the mobility functions to the edge of the network bringing it closer to the users. Its ultimate goal is to allow mobility anchor called Mobile Access Gateway (MAG), which is located at the edge of the network, and handles the mobility signaling and data routing through tunnel creation without any centralized node's assistance.

In the 5G network infrastructure where access network points are very densely deployed, the DMM protocol is a promising candidate for mobility management because of its flat and flexible mobility architecture [13]. However, in spite of its clear advantage for efficient traffic delivery in 5G network [14], this solution must be equipped with a dedicated security protocol that can defend various threats such as impersonation, denial-of-service, man-in-the-middle attacks. With just a few of researches [15]–[18], the DMM solution still has no major security protocol, thereby heavily counting on the layer 2 security which cannot address well the specified attacks listed in Table 1. Consequently, implementing an effective security countermeasure is essential considering that attackers are becoming more innovative. Motivated by this, we propose a secure and efficient protocol for DMM networks that supports mutual authentication, key agreement, confidentiality, integrity, and privacy while defending against DMM-specified attacks. The main contributions of this paper are as follows:

- We design a security protocol for the DMM networks based on the 5G network entities.
- We thoroughly verify the correctness of the proposed protocol in a formal way using the two popular security analysis tools, BAN-logic [19] and Automated Validation of Internet Security Protocol and Application (AVISPA) [20].
- We conduct a comparison analysis between our proposed protocol against contemporary security protocol standards including EAP-AKA [21], EAP-TLS [22], EAP-IKEv2 [23] and other proposed works.

The remainder of this paper is organized as follow. We first discuss the basic concept of the DMM protocol and its related attacks in Section II, followed existing security schemes and the Extensible Authentication Protocol (EAP) framework [24], which is a major network security scheme. Then, Section III discusses in detail our proposed protocol, which is formally verified in Section IV. The comparison result of our

TABLE 1. Security threats of PMIPv6-based DMM solution.

Channel	Message	Threat	Effect	Counter Measure
MN-MAG	Router Solicitation	Session Hijacking	Attackers hijack a session by impersonating an authorized MN.	Message Protect Mutual Authentication
	Router Advertisement	Denial of Service	Attackers causes a victim MN to configure incorrect network information.	Message Protect
CMD-MAG	PBU / PBA MCReq / MCRes	Attack by malicious MAG	(1) Messages are protected, but when a MAG collapses, variety of cyber-attacks can happen. (2) A collapsed MAG can launch redirection attack where data traffic intended for a victim MN is directed to itself.	Commitment of MN to handover must be verified separately.
		Attack by malicious CMD	If a CMD collapses, it may try redirection attack by sending a PBU to the MAGs associated with the current MN.	
MAG-MAG	BU / BA	Attack by malicious MAG	Messages are protected, but when MAG collapses, variety of cyber-attacks can happen.	Commitment of MN to handover must be verified separately.

approach against some security standards and existing works is presented in Section V. Finally, we summarize our work and present our future works in Section VI.

II. RELATED WORKS

This section discusses related works which is divided into four parts: the concepts of DMM and solutions, the vulnerabilities of PMIPv6-based DMM variants, DMM security, and EAP framework.

A. DISTRIBUTED IP MOBILITY MANAGEMENT

DMM is based on flat architecture aiming to push the location management functions and traffic routing to the network access level as illustrated in Figure 3.

As mentioned above, a MAG[1] serves as access router that supports address allocation function and location management. Once MN moves to another serving network, a new MAG (MAG2) not only allocates a network prefix to that MN but also disseminate MN's location information to the old MAG (MAG1) by sending location update signaling message. Such a handover leads to an establishment of a bi-directional tunnel, over which a data traffic intended for MN is forwarded from the old MAG to the new MAG. This configuration clearly enables the separation of the data plane and the control plane Furthermore, a better traffic load balance is achieved through the decentralization of the data plane.

In DMM networks, there are two suggested deployment options; partially distributed or fully distributed model [25]. In the former, there exists a centralized controller which is responsible for all control plane functions while relieving itself from route management and data forwarding, whereas the latter implements both functions at a customized network access hardware. To support distributed management, two notable DMM protocols were proposed in [13] and [14], which inherits several attributes from the conventional IP mobility protocol known as PMIPv6. Both protocols adopt the partially distributed model where the centralized LMA is replaced with Control Mobility Database (CMD). The two variants differ in message exchange but both end-up establishing bi-directional tunnel between MAGs as illustrated in Figure 2. Even though both protocols can create tunnel for data security, they still face security threats like impersonation attack, denial-of-service, and attacks initiated by compromised MAG and CMD.

B. VULNERABILITES OF PMIPV6-BASED DMM

An illustration of attack scenario corresponding to the PMIPv6-based DMM variants is presented in Figure 4. A MAG starts an attachment procedure when it receives a Router Solicitation (RS) message from a MN. As show in Figure 4a, if the RS message is not protected, a man-in-the middle attacker can capture the message and use it to impersonate the victim MN. As a result, the attacker can hijack the session established between the victim MN and the serving MAG. Furthermore, after a MAG finishes the attachment procedure, it finally transmits a Router Advertisement (RA) message to a MN. As depicted in Figure 4b, if an attacker somehow manipulates this RA message to include malicious network information, the victim MN can be deceived into configuring itself wrongly, thereby hindered from enjoying any service from the network. Additionally, the protocol of [13] and [14] are also vulnerable to attacks launched by malicious MAGs as shown in Figure 4c and 4d. A malicious MAG can deceive CMD or MAG with fake binding update messages of MN. 4c's attack scenario corresponds to the protocol in Figure 3a. In this scenario, the malicious MAG can mislead the CMD by sending a bogus Proxy Binding Update (PBU) message. Once the messaged is approved, the CMD then derives new PBU messages from the bogus

[1] The MAG can also be called *Mobile Anchor and Access Router (MAAR)*

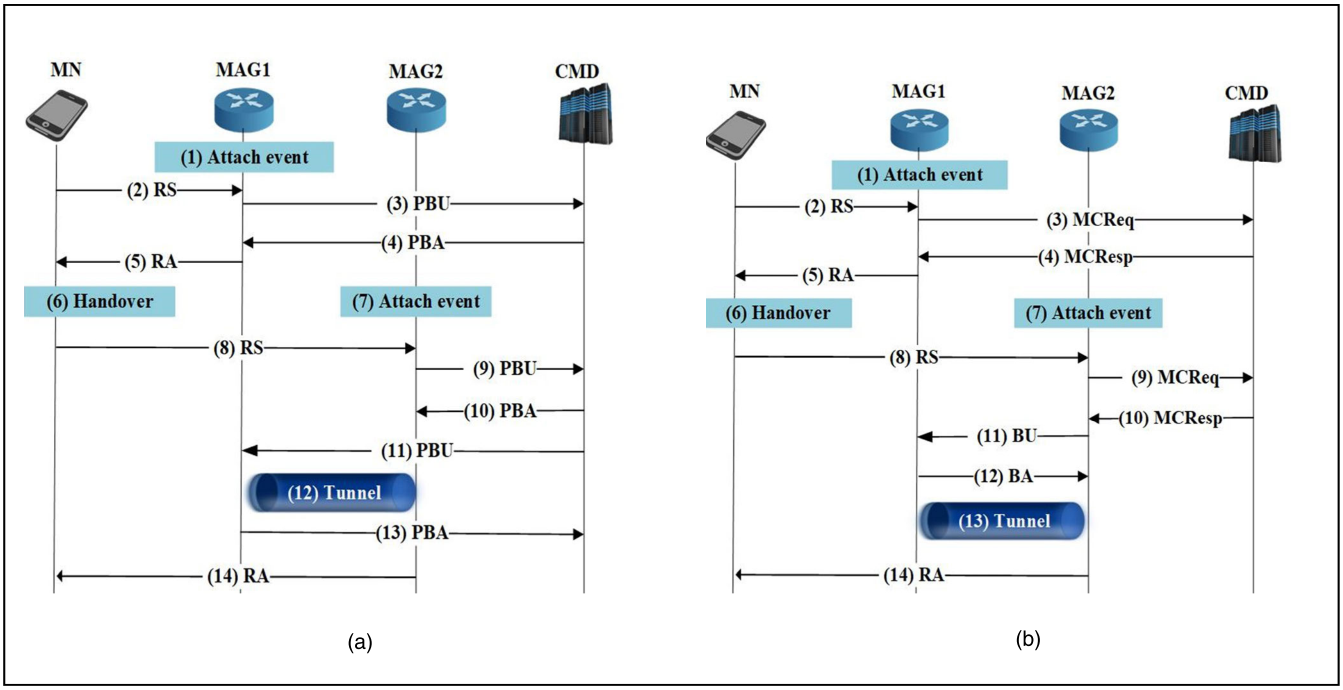


FIGURE 2. The message exchange sequence of PMIPv6-based DMM variants where (a) is from [14] and (b) from [15].

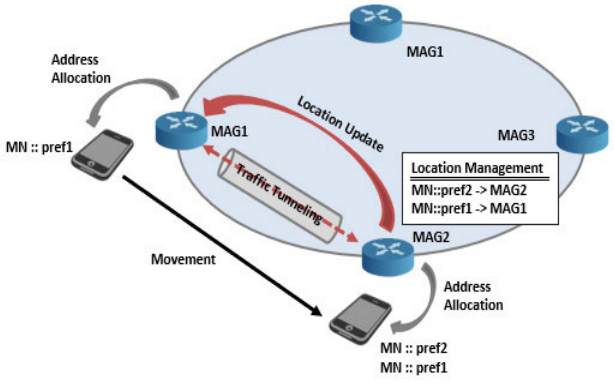


FIGURE 3. Fully Distributed Mobility Management Model.

one, which are then transmitted to the involved MAGs. As a result, the victim's data traffics are unintentionally transmitted. On the other hand, in case of Figure 4d, an attacker succeeds in deceiving CMD by sending and receiving the Mobility Context Request (MCReq) and Response (MCRes) messages, he or she can trick the involved MAGs by sending the malicious Binding Update (BU) messages to them. Hence, if these BU messages are accepted by the involved MAGs, all data traffic will be redirected to the attacker or victims. The summary of the threat implication for PMIPv6-based DMM solutions is shown in Table 1 where a countermeasure to its corresponding threat is also suggested.

C. PMIPv6-BASED DMM SECURITY

In order to secure DMM protocols, several researches have been conducted as follows. Shin *et al.* [15] proposed a secure route optimization (RO) protocol for DMM-based smart home systems, which includes RO initialization and handover phase. Since the proposed protocol only considered route optimization security, it cannot be viewed as a general solution for other DMM network services. In [16], Lee introduced a secure authentication protocol based on his previously proposed PMIPv6-based DMM protocol [14]. The security protocol utilizes the ID-based mutual authentication between a MN and a MAG with key agreement on elliptic curve. The security association among the MN and MAG is successfully established with the assistance of an Authentication Server (AS). However, a malicious MAG can still deceive the involved MAGs about the mobility context of the victim MN since the message exchange sequence in this security protocol is simply patterned from the previous one. It still fails to confirm the willingness of MN for handover, hence, making the traffic redirection attack launched by compromised MAG feasible. Additionally, privacy of MN can be compromised since MN's long-term ID is send in plaintext. Moreover, the scheme still needs improvement as it adopts the conventional server-client model to authenticate the MN. All security contexts are derived in the AS and are then forwarded to the corresponding network entity. The author suggested a distributed peer-to-peer authentication approach. It is also worth noting that this work introduced a dynamic tunneling based on session-to-mobility ratio, hence reducing tunneling overhead among MAGs. Kim *et al.* [17] proposed the same authentication model as in [16] where the MN is authentication by an AS. The effectiveness of the proposed security proposed is also dependent on the assumption that all MAGs and CMD are honest. This assumption is too heavy as these network entities are also susceptible to attackers in

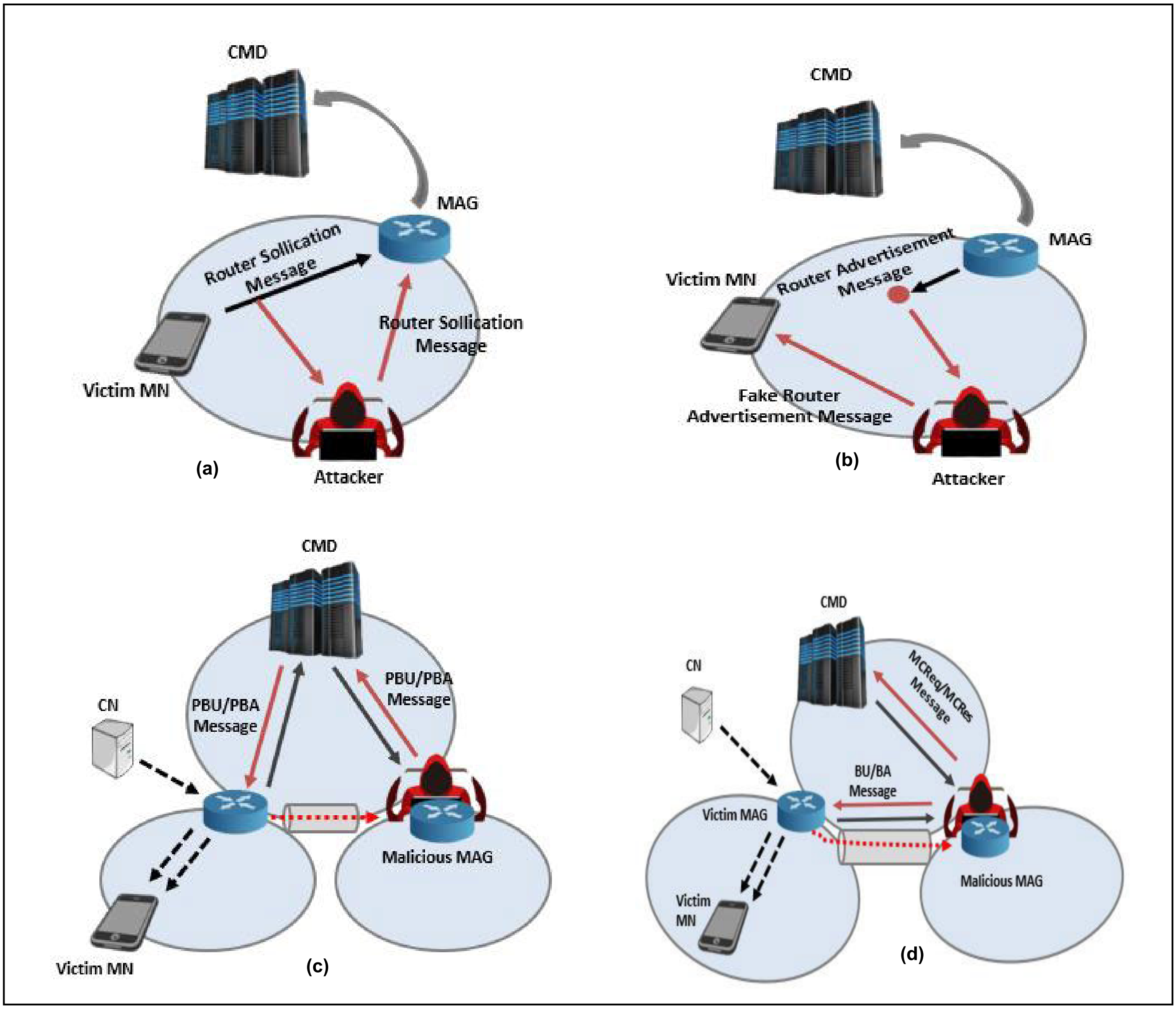


FIGURE 4. An illustration of the threats faced by PMIPv6-based DMM; (a) Impersonation attack (b) Denial-of-service, (c-d) attacks.

numerous situations. Along with these issues, the proposed protocol suffers the same problem in [16]. Moreover, both proposed security protocols were not formally verified by any verification tools. The proposed security protocol in [16] and [17] adopts a partially distributed management model where mobility signaling is managed by centralized node. To meet the requirements in a fully distributed management model under PMIPv6 domain, Vishal *et al.* [18] proposed a blockchain-based DMM scheme that uses three different blockchains namely PoW-wise, region-wise, and user-wise ledgers to overcome the security issues of the existing DMM solutions. However, the use of multiple ledgers may consume huge memory, considering also that frequent handovers are expected in the 5G networks. Additionally, the scheme could also affect the network performance. Moreover, it is not clear in this paper as to how the blockchains are completely managed by the different network nodes. In spite of the above security protocols, there is still no major security one DMM solutions. Accordingly, network operators tend to excessively rely on the layer network security which cannot adequately overcome the attacks listed in Table 2.

D. EAP FRAMEWORK

Alternatively, the EAP can be considered to protect DMM networks. The EAP has been known to be one of the most widely applied security frameworks for network security. It can provide high stability and scalability at authentication stage. Each entity can specify a supported EAP function and proceed with the agreed authentication procedures. The EAP framework is especially adopted as standard on the 5G network environment. Among its sub-security protocols, we focus on EAP method for 3rd Generation Authentication and Key Agreement (EAP-AKA) [21], EAP Transport Layer Security (EAP-TLS) [22], EAP Internet Key Exchange version 2 (EAP-IKEv2) [23] for comparison with our design.

TABLE 2. Notations.

Symbol	Description
MN	Mobile Node
AMF	Access and Mobility Management
CMDF	Central Mobility Database Function
IDs	X's ID
AID_i	The i-th anonymous ID
ADD_x	X's address
n_i	The i-th nonce
ts_i	The i-th timestamp
Kx	X's secret key
PR(X)	X's private key
HM_i	The i-th hash message
HMAC	Hash-based Message Authentication Code
SIG_x	Digital signature generated by X
HK	Handover key
SK	Session key
$\oplus$	Exclusive-OR operation

III. ENVIRONMENT AND PROPOSED PROTOCOL

This section describes the target environment and the details of the proposed security protocol. Table 2 gives abbreviations and notations which are used in the rest of this paper.

A. TARGET ENVIRONMENT

The target environment, which is depicted in Figure 5, is based on 5G stand-alone networks whose serving network is composed of three core functions: AMF, SMF, and UPF. To apply DMM to 5G stand-alone networks, each MAG can be divided into these three functions, where AMF, SMF, and UPF are responsible for access and mobility management, session management, and data transfer respectively. Moreover, a new network function CMDF is employed to play the role of CMD. In our scenario, the target 5G network is composed of a home network including AUSF, ARPF, and CMDF and three serving networks where two 3GPP networks and one non-3GPP network exist. Note that N3IWF handles the mobility management operation in non-3GPP networks as AMF does so in 3GPP networks. In such environment, MNs can move freely from one access network to another.

B. PROPOSED PROTOCOL

A secure and efficient protocol, depicted in Figure 6, is proposed for distributed mobility management based on 5G networks.

The assumptions made on the proposed protocol are as follows:

- It is assumed that the Non-Access Stratum (NAS) and Radio Resource Control (RRC) setups were performed during the initial authentication.
- It is assumed that the involved entities MN, AMFs, and CMDF are time-synchronized.
- It is assumed that the two values AID_0 and K_{AMF}, generated by CMDF, are distributed to the MN and the AMFs in advance through a secure channel.

The target security requirements of the proposed protocol are as follows:

- **Mutual authentication:** During the handover process, the MN and the target AMF, *i.e.* AMF(i+1) should mutually authenticate each other.
- **Confidentiality:** Any unauthorized entity should not be able to read the content of the data transmitted over the open channel.
- **Integrity:** Any unauthorized entity should not be able to make any changes on the data transmitted over the open channel.
- **Key exchange:** The two parties, MN and AMF(i+1) should successfully negotiate session keys without any leakage.
- **Privacy:** The real identity of MN must not be revealed in the exchanged messages.
- **Defense against attacks by malicious AMF or CMDF:**The attack launched by any malicious AMF or CMDF should be addressed.

The proposed protocol shown in Figure 6 aims to achieve secure and efficient handover procedure as the MN moves from the AMF(i) to the AMF(i+1) with the help of the CMDF while satisfying the target security properties.

The detailed description of the proposed protocol is as follows:

(i) Before the handover is executed, the AMF(i) is assumed to possess the AID_i and the K_{AMF} obtained during the i-th handover. Note that the AID_0 and the K_{AMF} are security distributed to the MN and the AMF(0) during the initial attachment.

(1) Once the MN' movement is detected through a layer 2 trigger, the AMF(i) initiates the handover by sending the *HI* message that includes the parameters ID_{MN}, AID_i, and K_{AMF} to the target AMF(i+1) over a secure channel. Upon receipt of this message, the AMF(i+1) utilizes the given ID_{MN}, AIDi, and K_{AMF} to obtain AID(i+1) by computing AID(i+1) $= ID_{MN} \oplus h(K_{AMF} || AID_i)$.

(2) With the help layer 2, the MN obtains the ID_{AMF} and then prepares for the *AccAuthReq* message, which includes the two IDs AID_{i+1} and $ID_{AMF(i+1)}$, a randomly generated nonce n_1, timestamp ts_1, and the two HMAC values HM_1 and HM_2. The HM1 and HM2 values are computed based on $HMAC(K_{CMDF}, ID_{MN}||ID_{AMF(i+1)}||n_1||ts_1)$ and

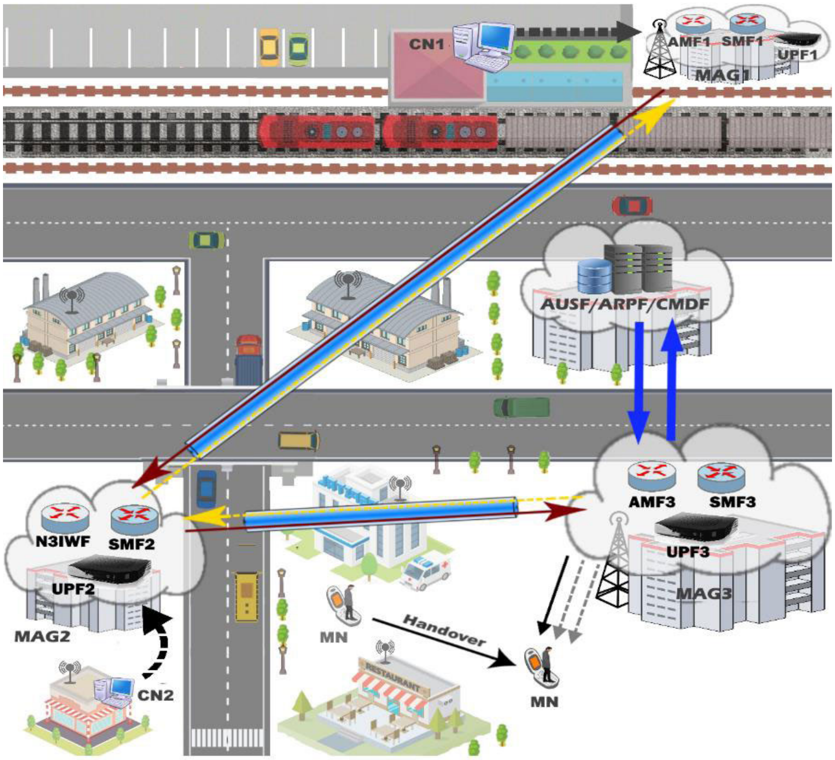


FIGURE 5. The scenario of the handover in 5G DMM.

HMAC(HK, *AccAuthReq*), respectively, where the handover key HK is computed as HMAC(KCMDF, $ID_{MN}||ID_{AMF(i+1)}||$" Handover Key"$||ts_1$). The *AccAuthReq* message is then transmitted to the $AMF_{(i+1)}$. Note that including the timestamp ts_1 in the calculation of HK ensures its freshness. It is also worth to note that the MN's privacy is maintained because only the temporary ID is shared in plaintext over the insecure channel. On receiving the *AccAuthReq message,* the AMF(i+1) first verifies the received ts_1 is within its accepted pre-defined time window. If the verification is positive, it retrieves the ID_{MN}, computes the HK, and verifies the *AccAuthReq* message by computing the HM_2 with the HK and comparing it with the received HM_2. The positive result indicates that the MN is reliable and consequently the AMF(i+1) can build trust with the MN. With such a trust, the AMF(i+1) proceeds to the step (3).

(3) In this step, the AMF(i+1) first makes the *MCReq* message with the MN's ID ID_{MN} and the received values $ID_{AMF(i+1)}$, n_1, ts_1, and HM_1, and in turn transmits that message to the CMDF through a secure channel. Upon receiving this message, the CMDF checks if the received timestamp ts_1 is within its time window and then proceeds to verifying the HM_1 through a pre-shared key K_{CDMF}. The positive verification of the HMAC value allows the CMDF to trust that the MN really intends to move to the AMF(i+1) because the K_{CMDF} is shared between only the MN and itself. In this way, if the AMF(i+1) is malicious, the CMDF can defend against the attacks by it.

(4)-(5) To proceed, the CMDF generates a random nonce n_2 and the timestamp ts_2, prior to computing the session key SK and the digital signature SIG_{CMDF} based on HMAC(K_{CMDF}, $ID_{MN}||ID_{AMF(i+1)}||$ "Session Key"$||n_1||n_2$) and E(PR(CMDF)), H(ID$||ADD_{AMF(i+1)}||ts_2$), respectively. The CMDF then prepares for the *MCRes* message, which includes the values n_1, n_2, ts_2, SK, a list of the AMFs, and SIG_{CMDF}. Here, the list contains the information of AMFs in the networks that were previously visited by the MN. Once the *MCRes* message arrives, the AMF(i+1) verifies the SIG_{CMDF} with the CMDF's public key after confirming if its handover request is correctly reflected on that signature. If the above verification is valid, the AMF(i+1) makes the Binding Update (BU) messages, each of which corresponds to each of the AMFs included in the received list of AMFs. Each *BU* message contains the received timestamp ts_2 and digital signature SIG_{CMDF}. Finally, the *BU* message are sent to their corresponding AMF.

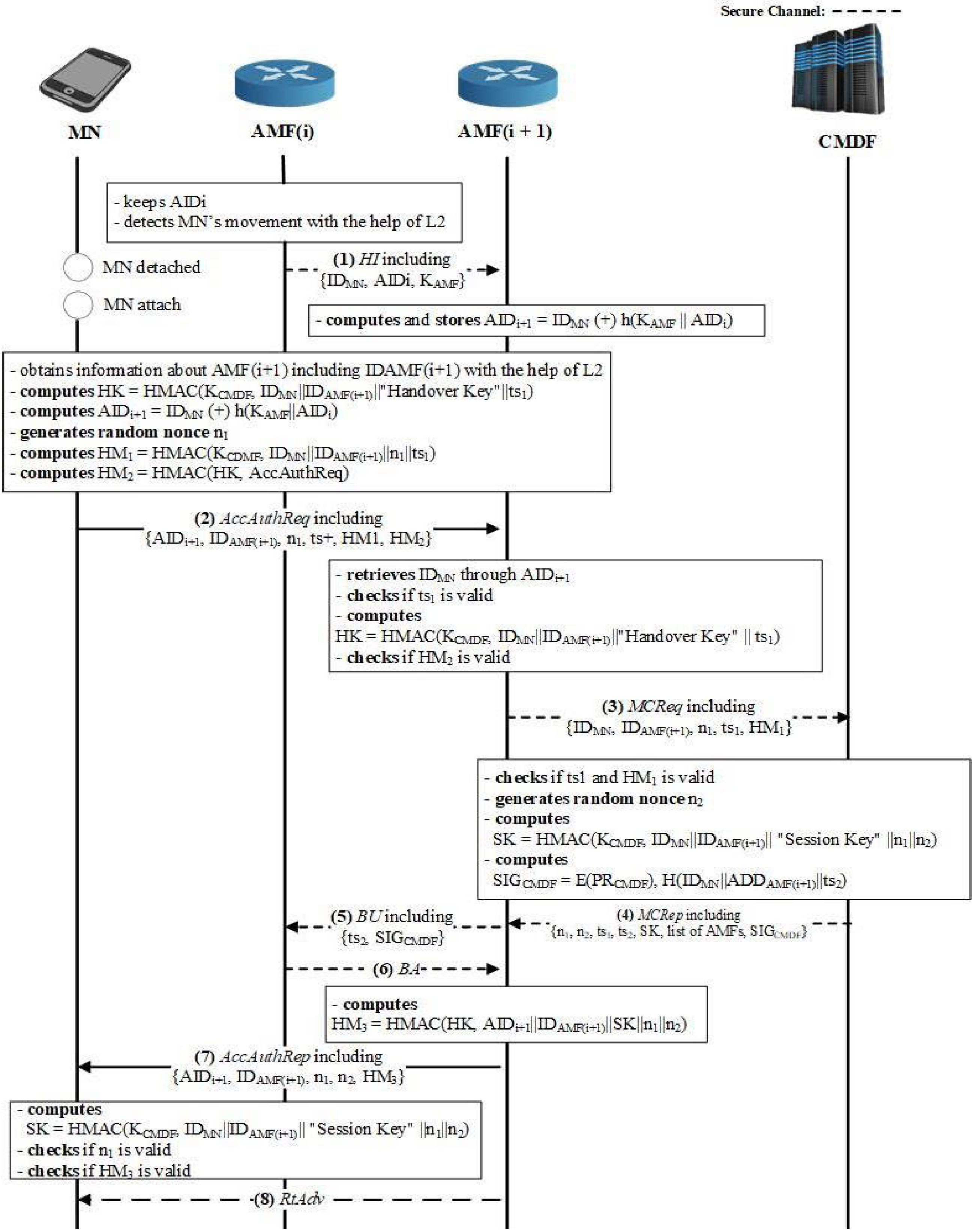

Secure Channel:
MN
AMF(i)
AMF(i + 1)
CMDF
- keeps AIDi
- detects MN's movement with the help of L2
MN detached
MN attach
(1) *HI* including
{ID_{MN}, AIDi, K_{AMF}}
- computes and stores $AID_{i+1} = ID_{MN}$ (+) h(K_{AMF} || AID_i)
- obtains information about AMF(i+1) including IDAMF(i+1) with the help of L2
- computes HK = HMAC(K_{CMDF}, ID_{MN}||$ID_{AMF(i+1)}$||"Handover Key"||ts_1)
- computes $AID_{i+1} = ID_{MN}$ (+) h(K_{AMF}||AID_i)
- generates random nonce n_1
- computes HM_1 = HMAC(K_{CDMF}, ID_{MN}||$ID_{AMF(i+1)}$||n_1||ts_1)
- computes HM_2 = HMAC(HK, AccAuthReq)
(2) *AccAuthReq* including
{AID_{i+1}, $ID_{AMF(i+1)}$, n_1, ts+, HM1, HM_2}
- retrieves ID_{MN} through AID_{i+1}
- checks if ts_1 is valid
- computes
HK = HMAC(K_{CMDF}, ID_{MN}||$ID_{AMF(i+1)}$||"Handover Key" || ts_1)
- checks if HM_2 is valid
(3) *MCReq* including
{ID_{MN}, $ID_{AMF(i+1)}$, n_1, ts_1, HM_1}
- checks if ts1 and HM_1 is valid
- generates random nonce n_2
- computes
SK = HMAC(K_{CMDF}, ID_{MN}||$ID_{AMF(i+1)}$|| "Session Key" ||n_1||n_2)
- computes
SIG_{CMDF} = E(PR_{CMDF}), H(ID_{MN}||$ADD_{AMF(i+1)}$||ts_2)
(5) *BU* including
{ts_2, SIG_{CMDF}}
(4) *MCRep* including
{n_1, n_2, ts_1, ts_2, SK, list of AMFs, SIG_{CMDF}}
(6) *BA*
- computes
HM_3 = HMAC(HK, AID_{i+1}||$ID_{AMF(i+1)}$||SK||n_1||n_2)
(7) *AccAuthRep* including
{AID_{i+1}, $ID_{AMF(i+1)}$, n_1, n_2, HM_3}
- computes
SK = HMAC(K_{CMDF}, ID_{MN}||$ID_{AMF(i+1)}$|| "Session Key" ||n_1||n_2)
- checks if n_1 is valid
- checks if HM_3 is valid
(8) *RtAdv*

FIGURE 6. The proposed protocol.

(6) Once receiving the *BU* message, the involved AMFs validate if the timestamp ts_2 is fresh and the digital signature SIG_{CMDF} is correct. Positive verification guarantees those AMFs the confidence in the MN's handover. Such a confidence derives them to complete the binding update by returning the Binding Acknowledgement (BA) message to the AMF(i+1). From this point, the MN's traffics are forwarded to the UPF(i+1) co-located at the AMF(i+1).

(7) After receiving the *BA* message from all the involved AMFs, the AMF(i+1) computes the HMAC HM_3 as $HMAC(HK, AID_{i+1}||ID_{AMF(i+1)}||SK||n_1||n_2)$, and in turn composes the *AccAuthRes* message together with AID_{i+1}, $ID_{AMF(i+1)}$, n_1, n_2, and the HMAC result. This message is then transmitted to the MN. Upon the message's arrival, the MN verifies if the received n_1 matches with the original one generated by itself which was included in the *AccAuthReq* message. If matched, replay attacks can be prevented because the nonce is proved to be fresh. Subsequently, the MN computes $HMAC(K_{CMDF}, ID_{MN}||ID_{AMF(i+1)}||\text{“Session Key”}||n1||n2)$ to get the session key SK, which is then used to verify the received HM_3. If the above verification is valid, we can see that the AMF(i+1) is authenticated to the MN and the SK is securely exchanged between these two parties.

(8) In parallel with sending the *AccAuthRes* message, the AMF(i+1) transmits the *RtAdv* one to the MN through a secure channel using the negotiated key SK. The MN sets up its network configuration with the information given by the received message.

IV. FORMAL VERIFICATION

This section presents the format verification of the proposed protocol under the two widely applied tools: BAN-logic [19] and AVISPA [20]. Applying these tools together can achieve more robust and thorough verification as they are considered to complement the weaknesses of each other.

A. FORMAL VERIFICATION WITH AVISPA

In AVISPA, target security protocols are verified by exploring their possible attacks, and can be regarded to be valid if no attack is found. For such a verification, a target protocol should be first modelled through the AVISPA's native script language High Level Protocol Specification Language (HLPSL), which as a role-based language configures each role independently as well as communications data between roles through channel. The structure of AVISPA is shown in figure 7. In other words, the protocol needs to be written in a form of HLPSL code. The written code is automatically converted to intermediate format (IF) by HLPSL2IF translator as depicted in Figure 7. The model is then analyzed by the 4 backend modules: On-the-Fly Model Checker (OFMC), CL-based Attacker Searcher (CL-AtSe) and SAT-based Model-Checker (SATMC), and Tree automate-based Protocol Analyzer (TA4SP).

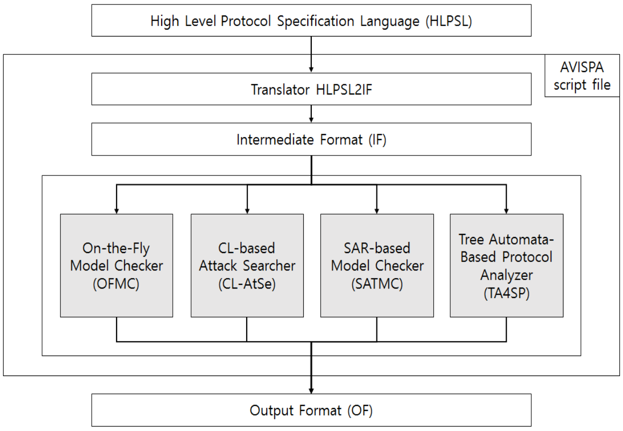
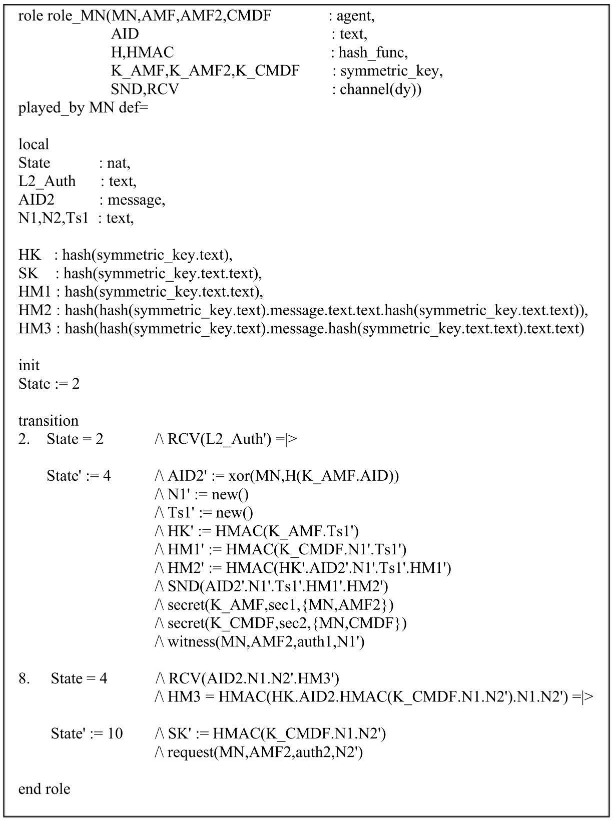

High Level Protocol Specification Language (HLPSL)
AVISPA script file
Translator HLPSL2IF
Intermediate Format (IF)
On-the-Fly Model Checker (OFMC)
CL-based Attack Searcher (CL-AtSe)
SAR-based Model Checker (SATMC)
Tree Automata-Based Protocol Analyzer (TA4SP)
Output Format (OF)

FIGURE 7. The structure of AVISPA.



```
role role_MN(MN,AMF,AMF2,CMDF                 : agent,
             AID                               : text,
             H,HMAC                            : hash_func,
             K_AMF,K_AMF2,K_CMDF               : symmetric_key,
             SND,RCV                           : channel(dy))
played_by MN def=

local
State        : nat,
L2_Auth      : text,
AID2         : message,
N1,N2,Ts1    : text,

HK   : hash(symmetric_key.text),
SK   : hash(symmetric_key.text.text),
HM1 : hash(symmetric_key.text.text),
HM2 : hash(hash(symmetric_key.text).message.text.text.hash(symmetric_key.text.text)),
HM3 : hash(hash(symmetric_key.text).message.hash(symmetric_key.text.text).text.text)

init
State := 2

transition
2.   State = 2          /\ RCV(L2_Auth') =|>

     State' := 4        /\ AID2' := xor(MN,H(K_AMF.AID))
                        /\ N1' := new()
                        /\ Ts1' := new()
                        /\ HK' := HMAC(K_AMF.Ts1')
                        /\ HM1' := HMAC(K_CMDF.N1'.Ts1')
                        /\ HM2' := HMAC(HK'.AID2'.N1'.Ts1'.HM1')
                        /\ SND(AID2'.N1'.Ts1'.HM1'.HM2')
                        /\ secret(K_AMF,sec1,{MN,AMF2})
                        /\ secret(K_CMDF,sec2,{MN,CMDF})
                        /\ witness(MN,AMF2,auth1,N1')

8.    State = 4         /\ RCV(AID2.N1.N2'.HM3')
                        /\ HM3 = HMAC(HK.AID2.HMAC(K_CMDF.N1.N2').N1.N2') =|>

      State' := 10      /\ SK' := HMAC(K_CMDF.N1.N2')
                        /\ request(MN,AMF2,auth2,N2')

end role
```

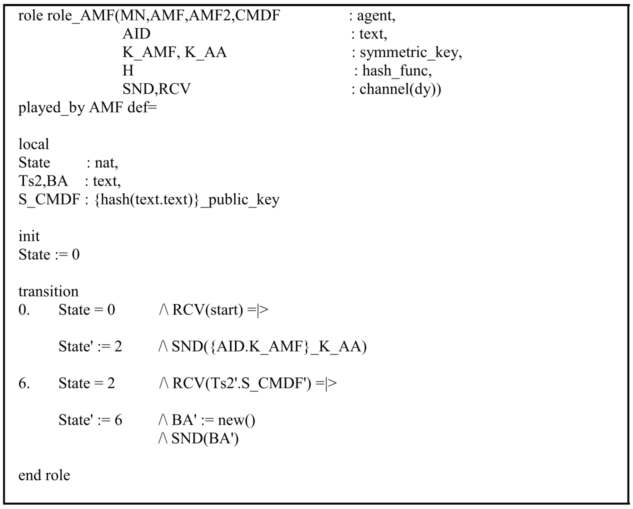
FIGURE 8. MN's basic role.

1) HLPSL MODEL

At first, each role is modeled in HLPSL code. The basic roles include the MN's role, the AMF1's role, the AMF2's role, and the CMDF's role as shown in Figures 8, 9, 10 and 11, respectively. Here, role_AMF1 and role_AMF2 corresponds to the model of previous and new AMF, respectively.

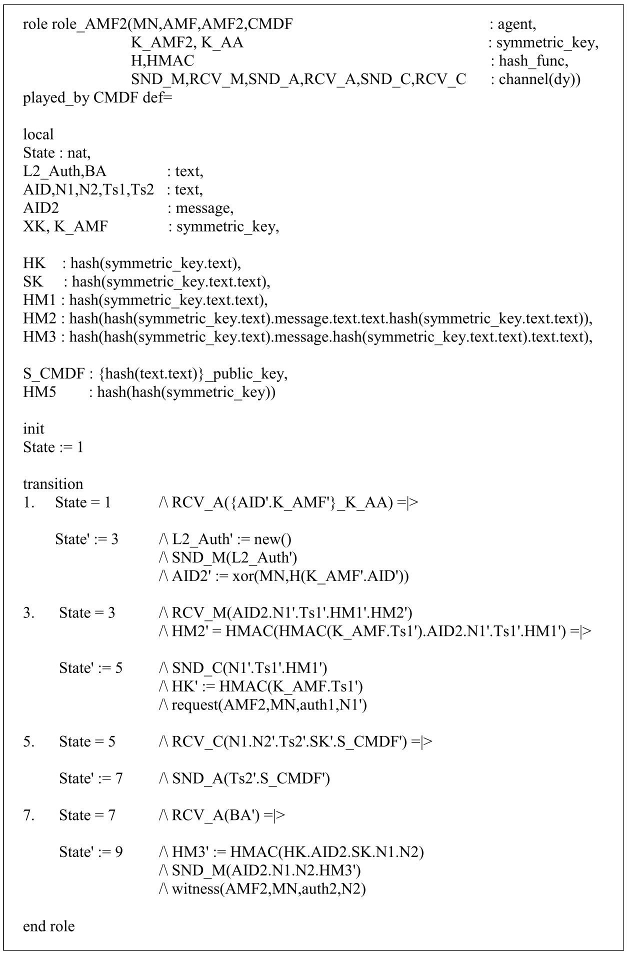
2) VERIFICATION RESULT

The obtained formal verification results, shown in Figure 12, are based on two back-end modules such as (a) OFMC and (b) CL-AtSe. The protocol's simulation diagram is illustrated in Figure 13. According to the results, the designed protocol is safe against known attacks.



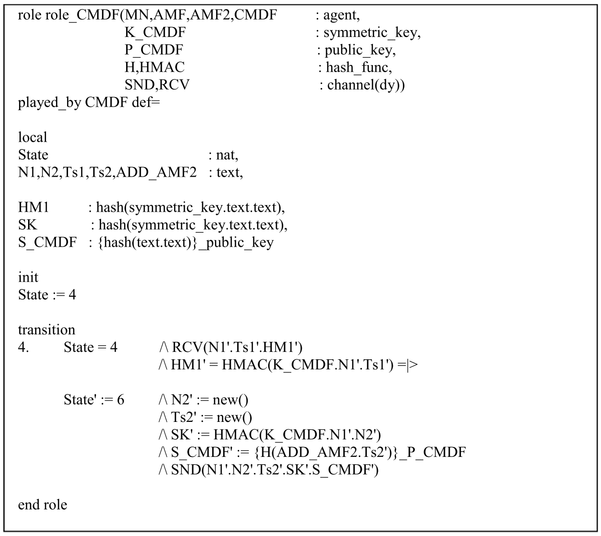
```
role role_AMF(MN,AMF,AMF2,CMDF          : agent,
              AID                        : text,
              K_AMF, K_AA                : symmetric_key,
              H                          : hash_func,
              SND,RCV                    : channel(dy))
played_by AMF def=

local
State      : nat,
Ts2,BA     : text,
S_CMDF : {hash(text.text)}_public_key

init
State := 0

transition
0.    State = 0       /\ RCV(start) =|>

      State' := 2     /\ SND({AID.K_AMF}_K_AA)

6.    State = 2       /\ RCV(Ts2'.S_CMDF') =|>

      State' := 6     /\ BA' := new()
                      /\ SND(BA')

end role
```

FIGURE 9. AMF1's basic role.



```
role role_AMF2(MN,AMF,AMF2,CMDF                              : agent,
               K_AMF2, K_AA                                  : symmetric_key,
               H,HMAC                                        : hash_func,
               SND_M,RCV_M,SND_A,RCV_A,SND_C,RCV_C           : channel(dy))
played_by CMDF def=

local
State : nat,
L2_Auth,BA           : text,
AID,N1,N2,Ts1,Ts2    : text,
AID2                 : message,
XK, K_AMF            : symmetric_key,

HK   : hash(symmetric_key.text),
SK   : hash(symmetric_key.text.text),
HM1 : hash(symmetric_key.text.text),
HM2 : hash(hash(symmetric_key.text).message.text.text.hash(symmetric_key.text.text)),
HM3 : hash(hash(symmetric_key.text).message.hash(symmetric_key.text.text).text.text),

S_CMDF : {hash(text.text)}_public_key,
HM5       : hash(hash(symmetric_key))

init
State := 1

transition
1.    State = 1        /\ RCV_A({AID'.K_AMF'}_K_AA) =|>

      State' := 3      /\ L2_Auth' := new()
                       /\ SND_M(L2_Auth')
                       /\ AID2' := xor(MN,H(K_AMF'.AID'))

3.     State = 3       /\ RCV_M(AID2.N1'.Ts1'.HM1'.HM2')
                       /\ HM2' = HMAC(HMAC(K_AMF.Ts1').AID2.N1'.Ts1'.HM1') =|>

       State' := 5     /\ SND_C(N1'.Ts1'.HM1')
                       /\ HK' := HMAC(K_AMF.Ts1')
                       /\ request(AMF2,MN,auth1,N1')

5.     State = 5       /\ RCV_C(N1.N2'.Ts2'.SK'.S_CMDF') =|>

       State' := 7     /\ SND_A(Ts2'.S_CMDF')

7.     State = 7       /\ RCV_A(BA') =|>

       State' := 9     /\ HM3' := HMAC(HK.AID2.SK.N1.N2)
                       /\ SND_M(AID2.N1.N2.HM3')
                       /\ witness(AMF2,MN,auth2,N2)

end role
```

FIGURE 10. AMF's basic role.



```
role role_CMDF(MN,AMF,AMF2,CMDF          : agent,
               K_CMDF                    : symmetric_key,
               P_CMDF                    : public_key,
               H,HMAC                    : hash_func,
               SND,RCV                   : channel(dy))
played_by CMDF def=

local
State                          : nat,
N1,N2,Ts1,Ts2,ADD_AMF2   : text,

HM1        : hash(symmetric_key.text.text),
SK          : hash(symmetric_key.text.text),
S_CMDF   : {hash(text.text)}_public_key

init
State := 4

transition
4.      State = 4        /\ RCV(N1'.Ts1'.HM1')
                         /\ HM1' = HMAC(K_CMDF.N1'.Ts1') =|>

        State' := 6      /\ N2' := new()
                         /\ Ts2' := new()
                         /\ SK' := HMAC(K_CMDF.N1'.N2')
                         /\ S_CMDF' := {H(ADD_AMF2.Ts2')}_P_CMDF
                         /\ SND(N1'.N2'.Ts2'.SK'.S_CMDF')

end role
```

FIGURE 11. CMDF's basic role.

B. FORMAL VERIFICATION WITH BAN-LOGIC

BAN logic, first introduced by Burrows *et al.* [19], has been widely adopted by security researchers and experts to formally verify security protocols. In this logic, to be formally verified, a target security protocol first needs to be translated into an idealized version, followed by defining its assumptions and goals. Afterwards, inference rules are applied repeatedly until the intended beliefs satisfying the goals are obtained. Tables 3 and 4 show the symbol, along with its meaning, and inference rules of BAN Logic, respectively.

In the first step, the protocol is expressed in an idealized form and the assumptions are made as shown in Figures 14 and 15, respectively. We skip the *BU* message because the AMF(i+1)'s belief derived from (I3), i.e., the belief on the $\mathrm{SIG}_{\mathrm{CMDF}}$, is semantically identical to what other involved AMFs can obtain from the $\mathrm{SIG}_{\mathrm{CMDF}}$ in the same way as the AMF(i+1) does.

From (I1), we derive:

(D1) $AMF\ (i+1)\ sees\ \langle ID_{MN}, ID_{AMF(i+1)}, n_1, ts_1\rangle_{HK}$

(D2) $AMF\ (i+1)\ believes$
$MNsaid\ \left[AID_{MN}, ID_{AMF(i+1)}, n_1, ts_1, HM\right]$
$by\ (D1), (A1), MM$

(D3) $AMF\ (i+1)\ believes\ MN\ believes$
$(AID_{MN}, ID_{AMF(i+1)}, n_1, ts_1, HM)$
$by\ (D2), (A2), FR, NV$

(D4) $AMF\ (i+1)\ believes\ MN\ believesID_{MN}$
$by\ (D3), BC$

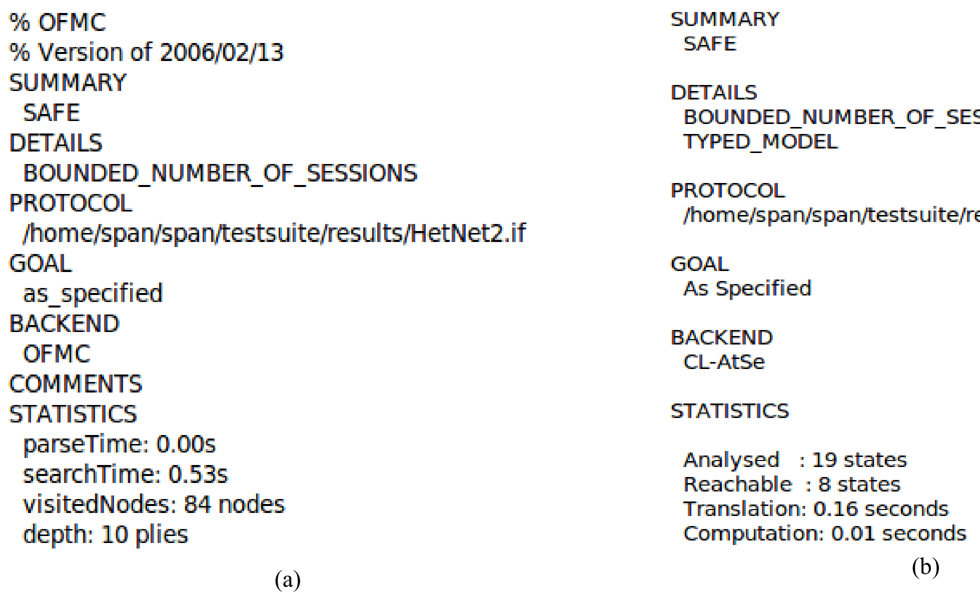
From (I2), we derive:

(D5) $CMDF\ sees\ \langle ID_{MN}, ID_{AMF(i+1)}n_1, ts_1\rangle_{K_{CMDF}}$

(D6) $CMDF\ believes\ MN\ said\ (ID_{MN}, ID_{AMF(i+1)}, n_1, ts_1)\ by\ (D5), (A3), MM$

(D7) $CMDF\ believes\ MN\ believes\ (ID_{MN}, ID_{AMF(i+1)}, n_1, ts_1) by\ (D6), (A4), FR, NV$

(D8) $CMDF\ believes\ MN\ believes\ (ID_{MN}, ID_{AMF(i+1)})\ by\ (D7), BC$



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/HetNet2.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.53s
  visitedNodes: 84 nodes
  depth: 10 plies
```

(a)

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/HetNet2.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 19 states
  Reachable  : 8 states
  Translation: 0.16 seconds
  Computation: 0.01 seconds
```

(b)

FIGURE 12. Formal verification result for handover (a) OFMC based, (b) CL-AtSe.

From (I3), we derive:

(D9) $AMF(i+1)\ sees\ \{ID_{MN}, ADD_{AMF(i+1)}, ts_2\}_{PU^{-1}(CMDF)}$

(D10) $AMF\ (i+1)\ believes\ CMDF\ said\ \left(ID_{MN}, ID_{AMF(i+1)}, ts_2\right)\ by\ (D9), (A5), MM$

(D11) $AMF(i+1)\ believes\ CMDF\ believes\ \left(ID_{MN}, ID_{AMF(i+1)}\right)\ by\ (D10), (A6), FR, NV, BC$

From (I4), we derive:

(D12) $MN\ sees\ \langle ID_{MN}, ID_{AMF(i+1)}, MN \overset{SK}{\longleftrightarrow} AMF(i+1)\rangle_{HK}$

(D13) $MN\ believes\ AMF(i+1) said\ [ID_{MN}, ID_{AMF(i+1)}, MN \overset{SK}{\longleftrightarrow} AMF(i+1)]\ by\ (D12), (A7), MM$

(D14) $MN\ believes\ AMF(i+1)\ believes\ [ID_{MN}, ID_{AMF(i+1)}, MN \overset{SK}{\longleftrightarrow} AMF(i+1)]\ by (D13), (A8), FR, NV$

(D15) $MN\ believes\ AMF(i+1)\ believes\ ID_{AMF(i+1)}\ by (D14), BC$

(D16) $MN\ believes\ AMF(i+1)\ believes\ MN \overset{SK}{\longleftrightarrow} AMF(i+1) by D(14), BC$

(D17) $MN\ believes\ MN \overset{SK}{\longleftrightarrow} AMF(i+1)\ by\ D(15), (A9), JR$

TABLE 3. Notations of BAN-logic.

Notation	Meaning
$P\ believes\ X$	P believes the message X and acts as if it is true
$P\ sees\ X$	P receives the message X
$P\ said\ X$	P previously sent the message X
$P\ controls\ X$	P has authority on X
$\#(X)$	X is fresh
$P \overset{K}{\leftrightarrow} Q$	K is a secret key shared between P and Q
$\overset{K}{\rightarrow} P$	K is the P's public key
$P \overset{K}{\Leftrightarrow} Q$	K is a shared secret between P and Q.
$\{X\}_K$	X is encrypted with K
$\langle X\rangle_K$	X is combined with a secret K

Based on the derived beliefs, we establish the following lemmas.

Lemma 1: The proposed protocol supports mutual authentication between the MN and the AMF(i+1).

Proof: The derived beliefs (D4) and (D15) show that the MN and the AMF(i+1) mutually authenticate each other. Thus, we can conclude that the lemma 1 is valid. □

Lemma 2: The proposed protocol can defend against the redirection attacks launched the malicious CMDF and AMF(i+1).

Proof: Based on (D8), the CMDF can confirm that the MN really intends to move to the AMF(i+1). That makes it possible for the CMDF to prevent any malicious AMF from launching redirection attacks by sending fake *MCReq* messages. On the other hand, based on (D11), the AMF(i+1) can confirm that the CMDF reflects the meaning of its *MCReq* message on the MN's binding update procedure and returns the *MCRep* message. Thus, the AMF(i+1) can detect the attempt for the malicious CMDF's redirection attack prior to sending the *BU* messages. Even though the *BU* message is

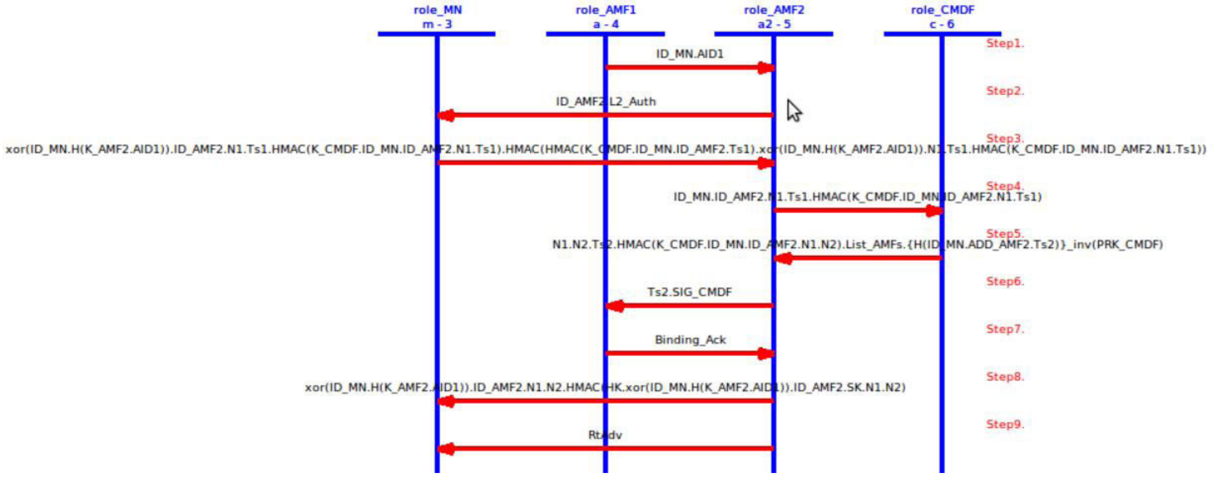

role_MN
m - 3
role_AMF1
a - 4
role_AMF2
a2 - 5
role_CMDF
c - 6
Step1.
ID_MN.AID1
Step2.
ID_AMF2.L2_Auth
Step3.
xor(ID_MN.H(K_AMF2.AID1)).ID_AMF2.N1.Ts1.HMAC(K_CMDF.ID_MN.ID_AMF2.N1.Ts1).HMAC(HMAC(K_CMDF.ID_MN.ID_AMF2.Ts1).xor(ID_MN.H(K_AMF2.AID1)).N1.Ts1.HMAC(K_CMDF.ID_MN.ID_AMF2.N1.Ts1))
Step4.
ID_MN.ID_AMF2.N1.Ts1.HMAC(K_CMDF.ID_MN.ID_AMF2.N1.Ts1)
Step5.
N1.N2.Ts2.HMAC(K_CMDF.ID_MN.ID_AMF2.N1.N2).List_AMFs.{H(ID_MN.ADD_AMF2.Ts2)}_inv(PRK_CMDF)
Step6.
Ts2.SIG_CMDF
Step7.
Binding_Ack
Step8.
xor(ID_MN.H(K_AMF2.AID1)).ID_AMF2.N1.N2.HMAC(HK.xor(ID_MN.H(K_AMF2.AID1)).ID_AMF2.SK.N1.N2)
Step9.
RtAdv

FIGURE 13. The protocol simulation.

TABLE 4. Rules of BAN-logic.

Rule	Formula
MM: Message Meaning Rule	$\dfrac{P\ believes\ P \overset{K}{\leftrightarrow} Q, P\ sees\ \{X\}_K}{P\ believes\ Q\ said\ X}$ $\dfrac{P\ believes\ P \overset{K}{\Leftrightarrow} Q, P\ sees\ \langle X\rangle_K}{P\ believes\ Q\ said\ X}$ $\dfrac{P\ believes\ \overset{K}{\rightarrow} Q, P\ sees\ \{X\}_{Q^{-1}}}{P\ believes\ Q\ said\ X}$
NV: Nonce Verification Rule	$\dfrac{P\ believes\ \#(X), P\ believes\ Q\ said\ X}{P\ believes\ Q\ believes\ X}$
JR: Jurisdiction Rule	$\dfrac{P\ believes\ Q\ controls\ X, P\ believes\ Q\ believes\ X}{P\ believes\ \ X}$
FR: Freshness Rule	$\dfrac{P\ believes\ \#(X)}{P\ believes\ \ \#(X,Y)}$
DR: Decomposition Rule	$\dfrac{P\ sees\ (X,Y)}{P\ sees\ X}$
BC: Belief Conjunction Rule	$\dfrac{P\ believes\ X, P\ believes\ Y}{P\ believes\ \ (X,Y)}$ $\dfrac{P\ believes\ Q\ believes\ (X,Y)}{P\ believes\ Q\ believes\ X}$ $\dfrac{P\ believes\ Q\ said\ (X,Y)}{P\ believes\ Q\ said\ X}$

not reasoned about, as the AMF(i+1) does, the AMFs in the MN's visiting networks can obtain the belief that the CMDF approves the MN's handover. Through this belief indirectly obtained from (D11), they can prevent the redirection attacks by the malicious AMF(i+1). As a result, it can be shown that the lemma 2 holds. □

Lemma 3: The MN and the AMF(i+1) has securely exchanged the session key SK.

$$(\text{I1})\ MN \rightarrow AMF(i+1){:}\ \langle ID_{MN}, ID_{AMF(i+1)}, n_1, ts_1, HM\rangle_{HK}$$
$$where\ HM = \left\langle ID_{MN}, ID_{AMF(i+1)}, n_1, ts_1\right\rangle_{K_{CMDF}}$$
$$(\text{I2})\ AMF(i+1) \rightarrow CMDF{:}\ \langle ID_{MN}, ID_{AMF(i+1)}, n_1, ts_1\rangle_{K_{CMDF}}$$
$$(\text{I3})\ CMDF \rightarrow AMF(i+1){:}\ \left\{ID_{MN}, ADD_{AMF(i+1)}, ts_2\right\}_{PU^{-1}(CMDF)}$$
$$(\text{I4})\ AMF(i+1) \rightarrow MN{:}\ \left\langle ID_{MN}, ID_{AMF(i+1)}, MN \overset{SK}{\leftrightarrow} AMF(i+1)\right\rangle_{HK}$$

FIGURE 14. Idealization.

$$(\text{A1})\ AMF(i+1)\ believes\ MN \overset{HK}{\leftrightarrow} AMF(i+1)$$
$$(\text{A2})\ AMF(i+1)\ believes\ fresh\ (ts_1)$$
$$(\text{A3})\ CMDF\ believes\ MN \xleftrightarrow{K_{CMDF}} CMDF$$
$$(\text{A4})\ CMDF\ believes\ fresh\ (ts_1)$$
$$(\text{A5})\ AMF(i+1) believes\ \xrightarrow{PU(CMDF)} CMDF$$
$$(\text{A6})\ AMF(i+1) believes\ fresh\ (ts_2)$$
$$(\text{A7})\ MN\ believes\ MN \overset{HK}{\leftrightarrow} AMF(i+1)$$
$$(\text{A8})\ MN\ believes\ fresh\ (MN \overset{SK}{\leftrightarrow} AMF(i+1)$$
$$(\text{A9})\ MN\ believes\ AMF(i+1)\ controls\ MN \overset{SK}{\leftrightarrow} AMF(i+1)$$

FIGURE 15. Assumptions.

Proof: From the AMF(i+1)'s point of view, in spite of no derived belief, it has an intuitive and direct belief on the authenticity of the session key SK since it securely receives that key from its trusted function CMDF over a pre-established secure channel. On the other hand, the MN has direct belief on the secure negotiation of the SK through (D17). This belief is intensified through (D16), which indicates that the MN enhances its belief on the SK by believing that the AMF(i+1) trusts the SK as well. Therefore, we can conclude that the lemma 3 is valid. □

Lemma 4: The protocol protects the MN's privacy.

Proof: Note that the path between the MN and the AMF(i+1) is not protected whereas other paths between the AMF(i) and the AMF(i+1) or between the AMF and the

CDMF are protected through pre-established secure channel. Therefore, we focus on the MN-AMF(i+1) path to check if the proposed protocol keeps the MN's privacy. Here, keeping the MN's privacy means that it is unable for outsiders to identify the MN. In the proposed protocol, for each handover, a new anonymous ID, *i.e.*, AID_i, is generated and assigned to the MN. Moreover, such an anonymous ID can be computed by only the MN and its visiting AMFs with their shared secret key K_{AMF}. Consequently, without knowing the K_{AMF}, it is almost impossible to extract the MN's ID ID_{MN} from the anonymous ID as well as trace the MN because its anonymous ID is changed in every handover. As a result, considering that in the MN-AMF(i+1) path, the MN's ID is hidden by replacing it with the anonymous ID, the proposed protocol can preserve the MN's privacy. □

Lemma 5: The proposed protocol support confidentiality and integrity

Proof: To support confidentiality, the session key SK must be securely negotiated between the involved entities. Notably, the lemma 3 shows that it is securely exchanged between the MN and the AMF(i+1). On the other hand, providing integrity can be proved by the beliefs derived from the HMAC values HM_1 to HM_3 and the signature SIG_{CDMF}. Accordingly, through the established beliefs (D3), (D7), (D11), and (D14), it shows that the integrity for the *AccAuthReq*, *MCReq*, *MCRep*, and *AccAuthRep* messages is achieved. As a result, we conclude that the lemma 4 is valid. □

Theorem 1: The proposed protocol is correct as well as satisfy the security requirements including confidentiality, integrity, mutual authentication, key exchange, privacy, and defense against redirection attacks by malicious node.

Proof: From the above derived beliefs (D1)-(D17), it can be shown that the proposed protocol is correct. Moreover, the obtained lemmas demonstrate that the proposed protocol satisfies the security requirements including confidentiality, integrity, mutual authentication, key exchange, privacy, and defense against redirection attacks by malicious node. □

V. COMPARATIVE ANALYSIS

This section presents the comparative evaluation results in terms of the following three aspects: security analysis, handover latency analysis, computation overhead. For comparison, we consider not only the DMM security protocols (Lee's protocol [16] and Kim *et al.*'s protocol [17]), but also the EAP based protocols including EAP-AKA [21], EAP-TLS [22], and EAP-IKEv2 [23], which are widely adopted security protocols in mobile and wireless networks.

A. SECURITY ANALYSIS

The proposed protocol is compared with other existing protocols in terms of the six security requirements. As shown in Table 5, the proposed protocol unlike others satisfies all the security requirements while in particular showing that it is specialized to DMM networks by supporting ⓔ and ⓕ.

TABLE 5. Comparison analysis on security property satisfaction.

Scheme	Security Features					
	ⓐ	ⓑ	ⓒ	ⓓ	ⓔ	ⓕ
[16]	✓	✓	✓	✓	×	×
[17]	✓	✓	✓	×	×	×
[21]	✓	✓	✓	✓	×	×
[22]	✓	✓	✓	✓	×	×
[23]	✓	✓	✓	✓	×	×
DMM-SEP	✓	✓	✓	✓	✓	✓

Note:

✓: Support, ×: Not Support, ⓐ: Confidentiality ⓑ: Integrity

ⓒ: Mutual Authentication ⓓ: Key Exchange ⓔ: Privacy

ⓕ: Defense against Redirection Attacks by Malicious Node

B. HANDOVER LATENCY ANALYSIS

In the different EAP authentication types considered in this paper, the full EAP exchange is required whenever the MN changes its point of attachment. Accordingly, the handover latency in EAP is derived as:

$$L_{HO-EAP} = L_{L2} + 2D_{nAMF-CMDF} + 2nD_{nAMF-pAMF} + L_{HO-AU} \quad (1)$$

where L_{L2}, which is dependent on the wireless chipset used, is the average latency at the link-layer. The $D_{nAMF-CMDF}$and the $D_{nAMF-pAMF}$ are the average delay for a message to arrive from the AMF to the CMDF, and between AMFs, respectively. The n refers to the number of AMFs that the MN has visited previously. L_{HO-AU} is the average time required to finish the EAP protocol. This value is expressed as:

$$L_{HO-AU} = 2D_{MN-nAMF} + D_{nAMF-AS} + T(m, T_{MN-AS}) \quad (2)$$

among which D_{MN-AMF} and $D_{nAMF-AS}$ are the average transmission delay between the MN and the AMF, and between the AMF and the AS. D(•) is the average latency function of a particular EAP scheme where m is the number of exchanged message between MN and AS. Note that D_{MN-AS} is equal to D_{MN-AMF}+ D_{AMF-AS} because all message from the MN are transmitted to the AS through the AMF.

In [16] and [17], whenever the MN moves to the target AMF, mutual authentication is executed in the same as how it was during the initial attachment. Consequently, their handover latency is expressed as:

$$L_{HO-DMM} = L_{L2} + 2D_{nAMF-CMDF} + 2nD_{nAMF-pAMF} + S_{HO-AU} \quad (3)$$

where S_{HO-AU} is the average latency of the authentication procedure during the initial attachment. This value is expressed as:

$$S_{HO-AU} = 2D_{MN-nAMF} + D_{nAMF-AS} + D_{MN-AS} \quad (4)$$

Furthermore, the handover latency of our proposed protocol is derived as:

$$L_{HO-PRO} = L_{L2} + 3D_{MN-nAMF} + 2D_{nAMF-CMDF} + 3nD_{nAMF-pAMF} \quad (5)$$

TABLE 6. The comparison of the proposed protocol and security protocols in terms of computation overhead.

Scheme	Computation Overhead				
	MN	AMF(i+1)	CMDF	AS	Total
LEE	$1C_{ECM} + 2C_{SHA1} + 2C_{HM} + 1C_{SYM}$	$1C_{SYM}$	-	$3C_{ECM} + 3C_{SHA1} + 2C_{HM}$	$6C_{ECM} + 5C_{SHA1} + 4C_{HM} + 2C_{SYM}$
KIM et.al.	$1C_{HM} + 2C_{SHA1}$	$1C_{HM}$	-	$1C_{HM}$	$3C_{HM} + 2C_{SHA1}$
EAP-AKA	$1C_{SHA1} + 8C_{HM} + 1C_{SYM}$	$1C_{SYM}$	-	$1C_{SHA1} + 8C_{HM}$	$2C_{SHA1} + 16C_{HM} + 2C_{SYM}$
EAP-TLS	$1C_{CV} + 1C_{AS} + 1C_{SV} + 3C_{HM} + 2C_{SHA1} + 1C_{SYM}$	$1C_{SYM}$	-	$1C_{CV} + 1C_{AS} + 1C_{DS} + 3C_{HM} + 2C_{SHA1}$	$2C_{CV} + 2C_{AS} + 1C_{SV} + 1C_{DS} + 6C_{HM} + 4C_{SHA1} + 2C_{SYM}$
EAP-IKEv2	$1C_{DH} + 1C_{HM} + 1C_{DS} + 1C_{SV} + 3C_{SYM}$	$1C_{SYM}$	-	$1C_{DH} + 1C_{HM} + 1C_{DS} + 1C_{SV} + 2C_{SYM}$	$2C_{DH}+2C_{HM} + 2C_{DS} + 2C_{SV} + 6C_{SYM}$
DMM-SEP	$5C_{HM} + 1C_{SHA1} + 1C_{XOR} + 1C_{SYM}$	$3C_{HM} + 2C_{SHA1} + 1C_{XOR} + 1C_{SV} + 1C_{SYM}$	$2C_{HM} + 1C_{SHA1} + 1C_{DS}$	-	$10C_{HM} + 4C_{SHA1} + 2C_{XOR} + 1C_{SV} + 1C_{DS} + 2C_{SYM}$

Note:

- C_{SYM} : cost for performing a symmetric encryption/decryption
- C_{AS} : cost for performing an asymmetric encryption/decryption
- C_{DS} : cost for performing a digital signature
- C_{SV} : cost for performing a signature validation
- C_{DH} : cost for performing a Diffie-Hellman operation
- C_{HM} : cost for performing a HMAC function
- C_{SHA1} : cost for performing a SHA1 function
- C_{CV} : cost for performing a certificate validation
- C_{XOR} : cost for performing XOR-operation
- C_{ECM} : cost for performing elliptic-curve point multiplication

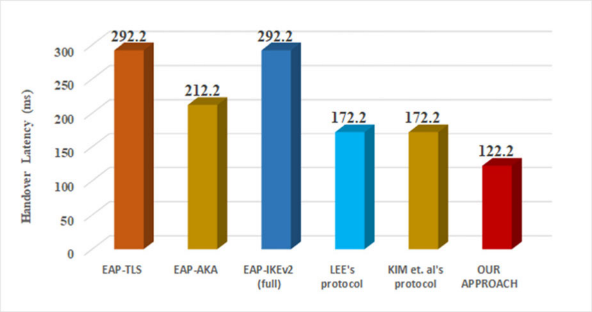


FIGURE 16. Handover latency (*ms*).

For comparative analysis, we adopt the following parameters: the latency of one hop $t_{HOP} = 10$ *ms* [26], $D_{MN-nAMF} = t_{HOP}$, $D_{nAMF-CMDF} = D_{nAMF-AS} = pt_{HOP}$ where p is the number of hops between the AMF and the CMDF/AS. We use $p = 3$ [27], and $L_{L2} = 2.2$ *ms* [26]. Additionally, m is set as 2, 4, and 4 for EAP-AKA [21], EAP-TLS [22], and EAP-IKEv2 [23], respectively.

Figure 16 shows the handover latency of the three EAP protocols, LEE's protocol, KIM *et al.*'s protocol, and our proposed protocol. As presented, the handover latency of the EAP protocols are higher than those of the other ones. This is because it requires to perform authentication procedure in the same way during the initial attachment, which results in high signaling overhead. On the other hand, the LEE's and KIM *et al.*'s protocols have similar handover latency because they follow the same authentication signaling sequence but slightly differ on the message content. Meanwhile, the proposed protocol has the smallest handover latency. This result is due to the customization of authentication procedure for the handover event.

C. COMPUTATION OVERHEAD

In this subsection, Table 6 presents the comparison of our proposed protocol against the schemes of Lee [16] and Kim and Shin [17] as well as three security standards under EAP framework [21]–[23] with respect to computation cost. Compared to EAP-TLS and EAP-IKEv2, the proposed protocol is more efficient because it allows MN to avoid asymmetric key operations. On the other hand, the protocol has higher computation cost than those of EAP-AKA, Lee's scheme, and Kim et. al.'s scheme. That is why it sacrifices efficiency to gain strong security enough to keep a reasonable trade-off between computational efficiency and handover security robustness. As a result, the proposed protocol achieves the strongest security with good computational efficiency.

VI. CONCLUSION

In 5G networks, it is very important to provide a secure and efficient handover because handover can happen frequently. For this reason, the DMM protocol was introduced, but current researches on DMM mostly concentrate on developing solutions for handover and data routing efficiency. Consequently, there has been lack of addressing security aspects, resulting in several security threats including the redirection attacks launched by malicious AMF or CMDF. Motivated by this, we proposed a secure and efficient handover protocol based on DMM architecture for 5G standalone network. For the proposed protocol, a mapping of the 5G standalone network entities to the DMM entities was first introduced. Moreover, the correctness of the proposed protocol was thoroughly proven by using formal verification tools BAN-logic and AVISPA. Based on the derived lemmas, it can be concluded that the proposed protocol supports mutual authentication, secure key exchange, integrity, confidentiality, and privacy in addition to defending against the redirection attacks by malicious AMF or CMDF. Finally, we showed in our comparative analysis that the proposed protocol is better in terms of security, handover latency, and computation overhead. In the future, we wish to implement the protocol in a real testbed but not limited to 5G architecture.

REFERENCES

[1] R. Q. Hu and Y. Qian, "An energy efficient and spectrum efficient wireless heterogeneous network framework for 5G systems," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 94–101, May 2014.

[2] X. Ge, S. Tu, G. Mao, C.-X. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 72–79, Feb. 2016.

[3] D. Johnson, C. Perkins, and J. Arkko, *Mobility Support in IPv6*, document RFC 3775, Jun. 2004.

[4] R. Koodli, *Fast Handovers for Mobile IPv6*, document RFC 4068, 2005.

[5] H. Soliman, C. Castelluccia, K. El Malki, and L. Bellier, *Hierarchical Mobile IPv6 Mobility Management (HMIPv6)*, document RFC 4140, Aug. 2005.

[6] H. Jung, E. Kim, J. Yi, and H. Lee, "A scheme for supporting fast handover in hierarchical mobile IPv6 networks," *ETRI J.*, vol. 27, no. 6, pp. 798–801, Dec. 2005.

[7] W. S. Hoh, S. Muthut, B.-L. Ong, M. Elshaikh, M. N. M. Warip, and R. B. Ahmad, "A survey of mobility management protocols," *ARPN J. Eng. Appl. Sci.*, vol. 10, no. 19, pp. 9015–9019, 2015.

[8] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, *Proxy Mobile IPv6 (PMIPv6)*, document RFC 5213, 2008.

[9] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, *Fast Handovers for Proxy Mobile IPv6*, document IETF RFC 5949, 2010.

[10] K. Sun and Y. Kim, "Flow mobility management in PMIPv6-based DMM (distributed mobility management) networks," *J. Wireless Mob. Netw., Ubiquitous Comput. Dependable Appl.*, vol. 5, no. 4, pp. 120–127, 2014.

[11] H. Chan, *Problem Statement for Distributed and Dynamic Mobility Management*, document draft-chan-distributed-mobility-ps-02, 2010.

[12] H. Chan, D. Liu, P. Seite, H. Yokota, and J. Korhonen, *Requirements for Distributed Mobility Management*, document RFC 7333, 2014.

[13] F. Giust, L. Cominardi, and C. Bernardos, "Distributed mobility management for future 5G networks: Overview and analysis of existing approaches," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 142–149, Jan. 2015.

[14] J.-H. Lee, J.-M. Bonnin, P. Seite, and H. Chan, "Distributed IP mobility management from the perspective of the IETF: Motivations, requirements, approaches, comparison, and challenges," *IEEE Wireless Commun.*, vol. 20, no. 5, pp. 159–168, Oct. 2013.

[15] D. Shin, K. Yun, J. Kim, P. V. Astillo, J.-N. Kim, and I. You, "A security protocol for route optimization in DMM-based smart home IoT networks," *IEEE Access*, vol. 7, pp. 142531–142550, 2019.

[16] J.-H. Lee, "Secure authentication with dynamic tunneling in distributed IP mobility management," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 38–43, Oct. 2016.

[17] D. Kim and Y. Shin, "An enhanced security authentication mechanism in the environment partially distributed mobility management," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, 2017, pp. 457–462.

[18] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and energy-efficient handover in fog networks using blockchain-based DMM," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 22–31, May 2018.

[19] 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.

[20] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganèo, and L. Vigneron, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. Int. Conf. Comput. Aided Verification*, 2005, pp. 281–285.

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

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

[23] 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 RFC 5106, 2008.

[24] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, *Extensible Authentication Protocol (EAP)*, document RFC 3748, 2004.

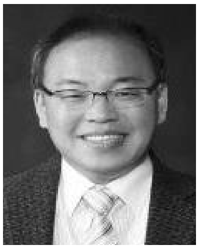
[25] P. Bertin, S. Bonjour, and J.-M. Bonnin, "A distributed dynamic mobility management scheme designed for flat IP architectures," in *Proc. New Technol., Mobility Secur.*, Nov. 2008, pp. 1–5.

[26] G. Brown, "New transport network architectures for 5G RAN: A heavy reading white paper," Fujitsu, Kanagawa, Japan, White Paper, 2018.

[27] I. You and J.-H. Lee, "SPFP: Ticket-based secure handover for fast proxy mobile IPv6 in 5G networks," *Comput. Netw.*, vol. 129, pp. 363–372, Dec. 2017.

JIYOON KIM received the B.S. and M.S. degrees in information security engineering from Soonchunhyang University, South Korea, in 2017 and 2019, respectively, where he is currently pursuing the Ph.D. degree. His current research interests include mobile internet security, 5G 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 was 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 of Clemson University, Clemson, SC, USA. His research interests include sensor development, embedded system design and development, mobile internet security, 5G security, and the IoT 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 an Associate Professor with the Department of Information Security Engineering, Soonchunhyang University, South Korea. His main research interests include 5G/6G security, the IoT security, authentication, access control, and formal security analysis. He is a Fellow of the IET. He is on the Editorial Board of *Information Sciences*, *Journal of Network and Computer Applications*, the *International Journal of Ad Hoc and Ubiquitous Computing*, *Computing and Informatics*, *Intelligent Automation and Soft Computing*, and so on. He is the Editor-in-Chief of *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, and *Journal of Internet Services and Information Security (JISIS)*.