IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 28, 2019, accepted September 15, 2019, date of publication September 26, 2019, date of current version October 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2943929

A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks

DAEMIN SHIN[1,2], KEON YUN[1], JIYOON KIM[1], PHILIP VIRGIL ASTILLO[1], JEONG-NYEO KIM[3], AND ILSUN YOU[1], (Senior Member, IEEE)

[1]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea
[2]Financial Security Institute, Yongin 16881, South Korea
[3]Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea

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

This work was supported in part by the Institute for Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korea Government (MSIT) under Grant 2018-0-00231, Development of context adaptive security autonomous enforcement technology to prevent spread of the IoT infrastructure attacks, and in part by the Soonchunhyang University Research Fund.

ABSTRACT Smart home networks have been recognized as one of its representative important applications in the forthcoming 5G era. It is also expected that in 5G networks, future smart home services will be much powered by mobility management, which enables users to remotely access and control their in-home Internet of Things (IoT) sensors and appliances anywhere anytime any device. As a major solution, Distributed IP Mobility Management (DMM) can be considered because it addresses the limitation of the centralized approaches as well as its flat architecture is suit for 5G networks. Obviously, without being protected, mobility management can cause smart home systems to be vulnerable to various security threats. Especially, it is of paramount important to protect data traffic transmitted between user mobile devices and their in-home IoT appliances because they include users' sensitive and critical privacy information. Taking this into consideration, it is necessary to support secure route optimization, which allows the involved devices to directly communicate each other in secure way while minimizing possibility of information leakage during data transmission. According to our best knowledge, there is no study on securing route optimization for DMM networks. Motivated by this, we propose a secure route optimization protocol for DMM-based smart home systems. The proposed security protocol, composed of the route optimization initialization and handover phases, is designed to provide mutual authentication, key exchange, perfect forward secrecy, and privacy protection. Its security is thoroughly verified through the two formal security analysis tools, BAN-logic and Automated Validation of Internet Security Protocols and Applications (AVISPA). From the comparison analysis, it is shown that the proposed protocol is better than other standard protocols.

INDEX TERMS Security, route optimization, distributed mobility management, smart home, IoT.

I. INTRODUCTION

Mobility management aims to enable each mobile node (MN) to get online regardless of its movement and location. With the advent of the 5G era, as expectations for innovative applications that go beyond existing limitations have increased, so its role as a key technology supporting these applications has become more and more important. Especially, mobility management is essential for emerging smart home networks which should support anytime, anywhere remote access to in-home Internet of Things (IoT) sensors and appliances by users' mobile devices. It is highly predicted that Distributed IP Mobility Management (DMM) [1], [2] will be adopted for the 5G networks and affiliated applications including smart home services. This is because its flat architecture is harmonized well with 5G networks while overcoming the critical shortcomings of the centralized mobility management technologies such as Mobile IPv6 [3] and Proxy Mobile IPv6 (PMIPv6) [4]. Accordingly, 5G smart home networks will count on DMM to allow MNs to remotely access and control their corresponding nodes (CNs), *i.e.*, in-home IoT sensors and appliances. On the other hand, needless to say, it is necessary to secure smart home networks, which can be otherwise faced with various security threats and attacks [5]–[12].

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

In particular, remote access can be the most critical attack target because it is easy to access and control devices inside smart home networks once security is compromised. Moreover, during remote access, users' sensitive privacy information are typically included in data transmitted over smart home networks. Therefore, to support remote access, user data should be sent as securely as possible through an optimized path without any intermediate nodes while accompanied by strong mutual authentication. In other words, secure route optimization is essential for smart home networks. In mobility management, several secure route optimization protocols were proposed for MIPv6 and PMIPv6 [3], [7], [13]–[17]. Especially, in [7], Shin et al. introduced a secure route optimization security protocol for smart home IoT networks. In this work, the proposed protocol relies on a centralized mobility anchor, based on PMIpv6 domain, to secure route optimization and manage seamless handover of MNs moving across different networks. A centralized approach is known to exhibit certain limitations such as scalability, single point of failure, etc. Accordingly, this paper acknowledges the DMM approach as solution to such problems. However, to take DMM into consideration, just few route optimization approaches were presented because it has not been yet finally standardized [18], [19]. More importantly, to our best knowledge, there is no security study on DMM route optimization. Motivated by this, we propose a security protocol for route optimization in DMM-based smart home IoT networks. The proposed protocol consisting of two phases is designed to provide mutual authentication, key exchange, perfect forward secrecy, and privacy while defending against the resource exhaustion and malicious insider attacks.

The contributions of this paper are three folds: (i) a secure route optimization for smart home IoT networks is proposed (ii) the proposed protocol is thoroughly verified with the two formal security verification tools, BAN-logic [20] and AVISPA [21], and (iii) comparison analysis is done in terms of security properties, computation overhead and communication overhead.

The rest of this paper is organized as follows. The section II provides both related works and problem statement. The proposed protocol is introduced and explained in the section III, and its formal verification is performed in the section IV. The comparison analysis is then presented in the section V, followed by the conclusion in the section VI.

II. RELATED WORKS AND PROBLEM STATEMENT

This section describes related studies, which are classified into three parts: smart home security, PMIPv6 route optimization, and DMM. The problem state is then described.

A. RELATED WORKS

1) SMART HOME SECURITY

In a smart home, it is necessary to secure the communication between in-home IoT devices and MNs. To this end, smart home security should thoroughly cover from data security to channel security. Especially, cloud computing can support such smart home security by deploying various platforms. Several researches have been conducted towards the smart home security as follows. Sivaraman et al. [22] focused on the security and privacy implications in the smart home IoT devices. The rating was discussed in terms of confidentiality, integrity, and access control, whose associated attacks were also highlighted. On the other hand, cloud-based platforms can act as the backbone of the future smart home while providing reliable and efficient services. Tao et al. [23] proposed a multilayer cloud architectural for reliable and efficient interactions between the heterogeneous IoT devices. The authors considered the ontology-based security framework for privacy and security in the interoperation of IoT devices. Chifor et al. [8] presented a device authorization scheme between smart home IoT devices and untrusted cloud systems. The authors not only adopted the Fast IDentity Online (FIDO) protocol for user authentication to the devices, but also maintained the user anonymity. Jacobsson and Davidsson [24] proposed a privacy and security model for smart homes whose security was discussed with recent advancements. Sicato et al. [25] highlighted the cyber-attacks on smart home devices and focused on the VPNfilter malware in a smart home. Furthermore, Ali and Awad [26] concentrated on the vulnerability assessment of IoT based on smart home and investigated risk mitigation approaches. The current generation smart homes and their networks are vulnerable to various kinds of attacks. Therefore, the single directional solutions towards security enhancements are not sufficient to secure them.

2) DISTRIBUTED IP MOBILITY MANAGEMENT

Nowadays centralized mobility management techniques including MIPv6 and PMIPv6 are mainly used in real worlds. However, these techniques have the following problems. First, all the traffics generated in MNs are concentrated to their anchor such as Home Agent (HA) or Local Mobility Anchor (LMA), which may cause network failure due to the overload of the anchor. Second, there is a limitation in expanding the network by increasing the load on the anchor because the amount of both signaling messages and data traffic exponentially increases in proportion to the number of MNs. Third, since data traffics are mainly transmitted through the anchor, such transmission can lead to an inefficient path such as triangular routing. In other words, centralized mobility management can provide convenience to mobility management in a hierarchical network structure, but there are performance or scalability issues, and anchors are the main cause of malicious attacks because all management is handled by a single anchor and easily targeted. To address these limitations, the IETF has launched the Distributed IP Mobility Management Working Group[1] since 2012 to standardize distributed Internet mobility management techniques.

[1] https://datatracker.ietf.org/group/dmm/about/

DMM distributes the centralized anchor's functionality to perform network functions independently in several places. For this goal, it is configured by separating the data plane (responsible for data traffic) and the control plane (responsible for signaling for mobility management). Decentralization of the data plane provides flexibility in the data flow, and reduces the probability of overload by not only preventing a single anchor from being focused on, but also distributing tunneling operations. Also, it can exhibit improved performance with low communication delay by excluding a centralized anchor from data transmission. Hence, it is highly expected that DMM will be a dominant mobility management standard for the next generation mobile networks, *i.e.*, the forthcoming 5G/6G networks. In particular, similar to Proxy Mobile IPv6 (PMIPv6) [4], network-based DMM gains considerable attentions because of running mobility management without MNs' involvement. In order to reduce anchor loads, this network-based approach centralizes and distributes the control and data planes respectively by employing Centralized Mobility Database (CMD), which stores and manages MNs' mobility information. Consequently, network-based DMM is adopted for our research.

3) ROUTE OPTIMIZATION SECURITY

Since the introduction to MIPv6, the first IPv6 mobility management solution, route optimization security has been one of important challenges. In MIPv6, the Return Routeability (RR) scheme is included as a basic route optimization security option. In spite of its simple structure and easy key management, this scheme contains fatal weaknesses in terms of security and performance. As an alternative to the RR protocol, the Enhanced Route Optimization (ERO) scheme was proposed and standardized [13]. The ERO scheme consists of the initial and subsequent stages. In the former, a binding management key is strongly exchanged based on address-based public-key encryption scheme named ''Cryptographically Generated Addresses (CGA),'' [27]. In the latter, a route optimization is efficiently executed based on the negotiated strong key. Moreover, the ERO scheme minimizes the binding update latency through the early binding update scheme, which simultaneously performs the binding update and data transfer. This creates a trade-off between performance and security. Basically, it is assumed in MIPv6 that there is no global security infrastructure and the two nodes MN and CN have no trust relation (the aforementioned RR and ERO are also designed under that assumption). However, in 2006, the Static Shared Key (SSK) scheme [14] was proposed as the route optimization standard in consideration of the case where there is a trust relationship between the involved MN and CN. Note that such a situation fits into our smart home environment because it is necessary to setup a pre-trust relationship for the involved entities. In this scheme, it is assumed that a shared secret is established between MN and CN in advance. Once a handover happens, an optimized binding update of one round-trip is executed based on the pre-shared key between the two nodes. However, the SSK scheme suffers from key distribution and management because each MN should directly establish trust relation in advance with its associated CN. In order to overcome this limitation, TBUA [15], a ticket-based binding renewal authentication protocol, was proposed. Especially it employs HA as a ticket issuer to address the burden on key distribution and management while adopting the early binding update to decrease the binding update latency. Afterwards, caTBUA [16] was proposed to enhance TBUA based on the context-aware authentication approach to keep the best balance between security and efficiency. Note that the schemes mentioned above aim to protect the route optimization of MIPv6, which is host based.

On the other hand, several schemes were proposed for the route optimization of PMIPv6, the current widely used mobility management standard [28], [29]. All of them focus only on communication efficiency, thus not satisfying the security requirements for smart home environments. In 2017, Shin et al. [7] presented the secure route optimization protocol for the PMIPv6 based smart home security, which achieves security and efficiency. As a potent successor of PMIPv6, DMM successfully has gained popularity, but still has not been standardized, thus leading to just a few of route optimization schemes [18], [19], whose focus is just on efficiency. To our best knowledge, there is no study on security for DMM route optimization, which is especially suit for smart home IoT networks. Clearly, based on the expectation that DMM will be the main mobility management scheme for 5G/6G networks, it is significant to research DMM route optimization and its security.

B. PROBLEM STATEMENT

The communication between MN and CN (*i.e.* in-home IoT device) in a basic DMM-based smart home IoT network is shown in Figure 1. Through two intermediary entities Mobility Gateway (MGW) and CMD, MN can communicate with CN regardless of its location and movement. In this smart home network, Home Gateway (HGW) is employed to serve as a bridge for communication between in-home IoT devices and external MNs. In more detail, all data traffics are transmitted between the associated MN and CN through tunneling generated between MGW and HGW. However, if MN moves to another network, its data traffics arrived at the old MGW or departed from the new MGW should be further forwarded between these two MGWs. Consequently, every time a handover occurs, such indirect routing degrades the overall network performance, leading to route optimization problems and excessive-performance loads. In order to address this problem, it is necessary to study the route optimization for DMM. On the other hand, the DMM- based smart home IoT network can be faced with various attacks such as redirection attack if its route optimization is not properly protected. In addition, data transmitted over smart home networks contains users' sensitive privacy information, whose leakage can result in fatal consequences. Accordingly, such data should

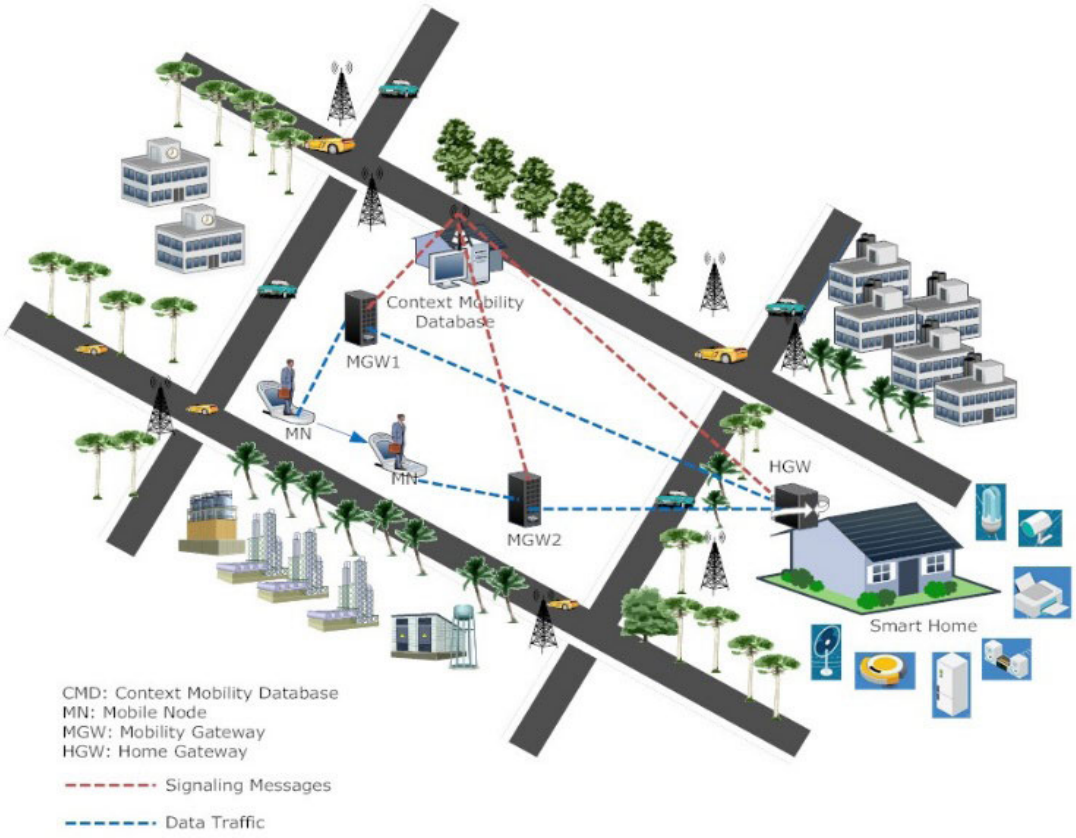


FIGURE 1. Smart Home Networks based on DMM.

be transmitted as securely as possible through an optimized path without any intermediate nodes, which means the truly secure route optimization. For that, the involved MGW and HGW should mutually authenticate each other while negotiating a master session key, from which sub-session keys are derived to protect the data traffics transmitted over smart home networks. Such security association should be established between new MGW and HGW whenever MN moves to new network. To support MGW and HGW to build their security association strong enough for the route optimization, we can take into consideration the well-known standard security protocols including EAP-TLS [30], EAP-AKA [31], EAP-IKEv2 [32], and so forth. Unfortunately, they cannot completely satisfy the security requirements specific for smart home networks, which are defined in the next section. That leads to us researching a new security protocol to protect the route optimization for DMM-based smart home IoT networks.

III. PROPOSED PROTOCOL

In this section, a secure route optimization protocol is proposed for DMM-based Smart Home IoT Networks. The proposed protocol includes two phases: the route optimization initialization (RO_INIT) and handover (RO_HO) phases. Table 1 shows the notations that are used in representing the proposed protocol.

TABLE 1. Notations.

Symbol	Description
MN	Mobile Node
CN	Corresponding Node
MGW	Mobility Gateway
MGW_i	The ith MGW
CMD	Context Mobility Database
HGW	Home Gateway
ID_X	ID of X
K_{MGWi}	Secret key between MGW_i and CMD
K_{HC}	Authentication key between HGW and CMD
K_{EHC}	Cipher key between HGW and CMD
n_i	The ith nonce
ts_i	The ith time stamp
T_{HGW}	Ticket issued by CMD to HGW
X, Y	Diffie-Hellman Private Key
g^X, g^Y	Diffie-Hellman Public Key
MSK_i	Master Session Key between MGW_i and HGW

The assumptions made on the proposed protocol are as follows:

- It is assumed that the mobile network operators to which MNs belong provides a smart home cloud service supporting distributed mobility management.
- It is assumed that the MN user subscribes to a smart home cloud service, thereby establishing a trust relation between her or his own home network and the

DMM-based mobile networks based on which that cloud service runs. In more detail, during the initial enrolment, the user's home gateway HGW shares the authentication and cipher keys, K_{HC} and K_{EHC}, with the context mobility database CMD in the DMM-based networks.

- It is assumed that during the initial enrolment, a route optimization policy is configured between each HGW and its corresponding DMM-based mobile networks.
- It is assumed that in DMM-based mobile networks, each MGW pre-establishes a secure channel with CMD based on the IPSec Encapsulating Security Payload (ESP) [33] in a way that the confidentiality and integrity of data being transferred are guaranteed.
- It is assumed that the communication between MGWs is protected by the pre-established IPSec ESP-based secure channel. Therefore, each MN's important handover and route optimization information are securely transmitted from the current MGW to the next MGW.

The proposed protocol targets the following security requirements:

- **Mutual Authentication**: For secure route optimization, HGW and MGW should mutually authenticate each other.
- **Key Exchange**: HGW and MGW should securely negotiate session keys to protect the route optimization process as well as the succeeding data transmission.
- **Perfect Forward Secrecy**: Since the security of data being transmitted between MN and CN is critical, the session key utilized to protect this transmission must support perfect forward secrecy. Even if the long term keys as well as the current and future session keys to be shared between HGW and CMD or between HGW and MGW are exposed, it must be impossible to recover the old session keys used to protect data from the past.
- **Privacy**: The MN's identity must not be revealed on the messages being exchanged between CMD and HGW or between MGW and HGW during the route optimization.
- **Defense against resource exhaustion attack**: Resource exhaustion attack is a kind of DoS attack that leads victims to an excessive utilization of its resources. The proposed protocol must not be vulnerable to DoS attack that causes the involved entities to suffer from expensive public key operations.
- **Defense against attacks by malicious MGW**: The proposed protocol must respond to the threat of re-direction attack by the malicious MGW.

In order to achieve the security requirements explained above, the proposed protocol protects the route optimization by performing session key exchange using the Diffie-Hellman protocol on the basis of the trust relationship between CMD and HGW.

A. ROUTE OPTIMIZATION INITIALIZATION PHASE (RO_INIT)

The RO_INIT phase, shown in Figure 2, aims to securely set up the router optimization between MN and its smart home network. For such a goal, this phase counts on the long term secret keys, K_{HC} and K_{EHC}, pre-shared between HGW and CMD. Assume that the communication between MN and CN, *i.e.*, smart home IoT device, via HGW is in progress prior to this phase. If MN has appropriate rights to participate in the route optimization, HGW monitors data traffics in order to make decision whether the route optimization is necessary or not. HGW starts the RO_INIT phase in the case that a route optimization is necessary. Once contacted by HGW, CMD checks the MN's route optimization policy to decide whether to proceed the requested route optimization or not. If available, it gets from its policy store both the HGW information (HGW address, K_{HC}, K_{EHC}, etc.) and the current MGW information (MGW address, K_{MGWi}, etc.), which are associated with MN.

The detailed description of this phase, outlined in Figure 2, is as follows.

1) Once deciding that a route optimization is necessary, HGW starts this phase by sending CMD the *HC_Auth_Req* message, which includes ID_{HGW} and $EMSG_1$. For this, HGW uses K_{EHC} to encrypt the values ID_{HGW}, ID_{MN}, n_1, ts_1 and HM_1 into $EMSG_1$ after preparing for the randomly generated nonce n_1 and the current timestamp ts_1 as well as computing $HM_1 = HMAC(K_{HC}, ID_{HGW}|| ID_{MN}||n_1||ts_1)$. Here, it is worth to note that the MN's privacy holds because ID_{MN} is encrypted. On receiving the message, CMD first gets the two secret keys K_{EHC} and K_{HC} through ID_{HGW}, and then decrypts $EMSG_1$ with K_{EHC}. Afterwards, it checks if ID_{HGW} and ID_{MN} are valid as well as ts_1 is within its time window, and verifies HM_1 with K_{HC}. If the above verification is positive, CMD successfully authenticates HGW based on the two keys K_{EHC} and K_{HC}. Moreover, it can defend against the reply attacks based on the ts_1's freshness.
2) After finishing to verify the the *HC_Auth_Req* message, CMD randomly generates n_2 and creates the session key K_{RO} by computing $HMAC(K_{HC}, n_1||n_2||$ "RO Init Key"), followed by issuing the ticket T_{HGW}. Finally, it computes $HM_2 = HMAC(K_{HC}, ID_{CMD}||ID_{MGW1}|| ID_{MN}||n_1||n_2||T_{HGW})$ prior to sending the *HC_Auth_Res* message to HGW. On arrival of the message, HGW verifies if the included n_1 matches the original one sent by itself and then HM_2 is valid. If the verification is successful, it can authenticate CMD as well as prevent the reply attack with the help of the n_1's freshness.
3) In order to prepare for the *HM_Auth_Req* message, HGW computes the session key K_{RO} and randomly generates the nonce n_3. It also creates its Diffie-Hellman private key X and calculates the corresponding public key g^X. After computing HM_3, it contacts

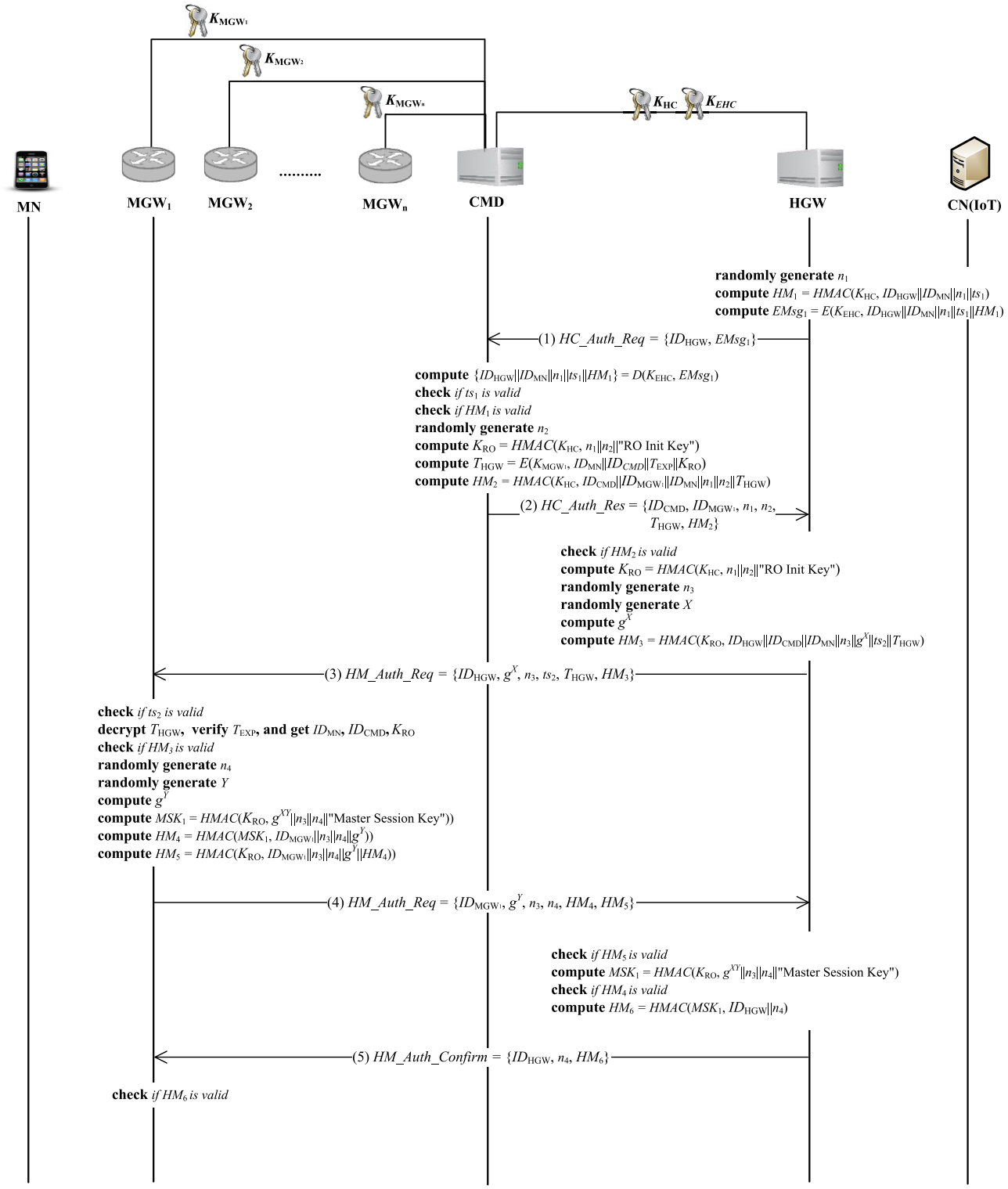


FIGURE 2. Route Optimization Initialization Phase (RO-INIT).

MGW_1 with the *HM_Auth_Req* message. On receiving this message, MGW_1 first checks if the included ts_2 is fresh, then decrypting the ticket T_{HGW} with K_{MGW1}. At this point, MGW_1 becomes aware that through the identifiers ID_{MN} and ID_{CMD}, this route optimization request is for MN and allowed by CMD. Moreover, it obtains the session key K_{RO} between HGW and itself, with which the included HM_3 is then verified. If HM_3 is valid, HGW is successfully authenticated to MGW_1.

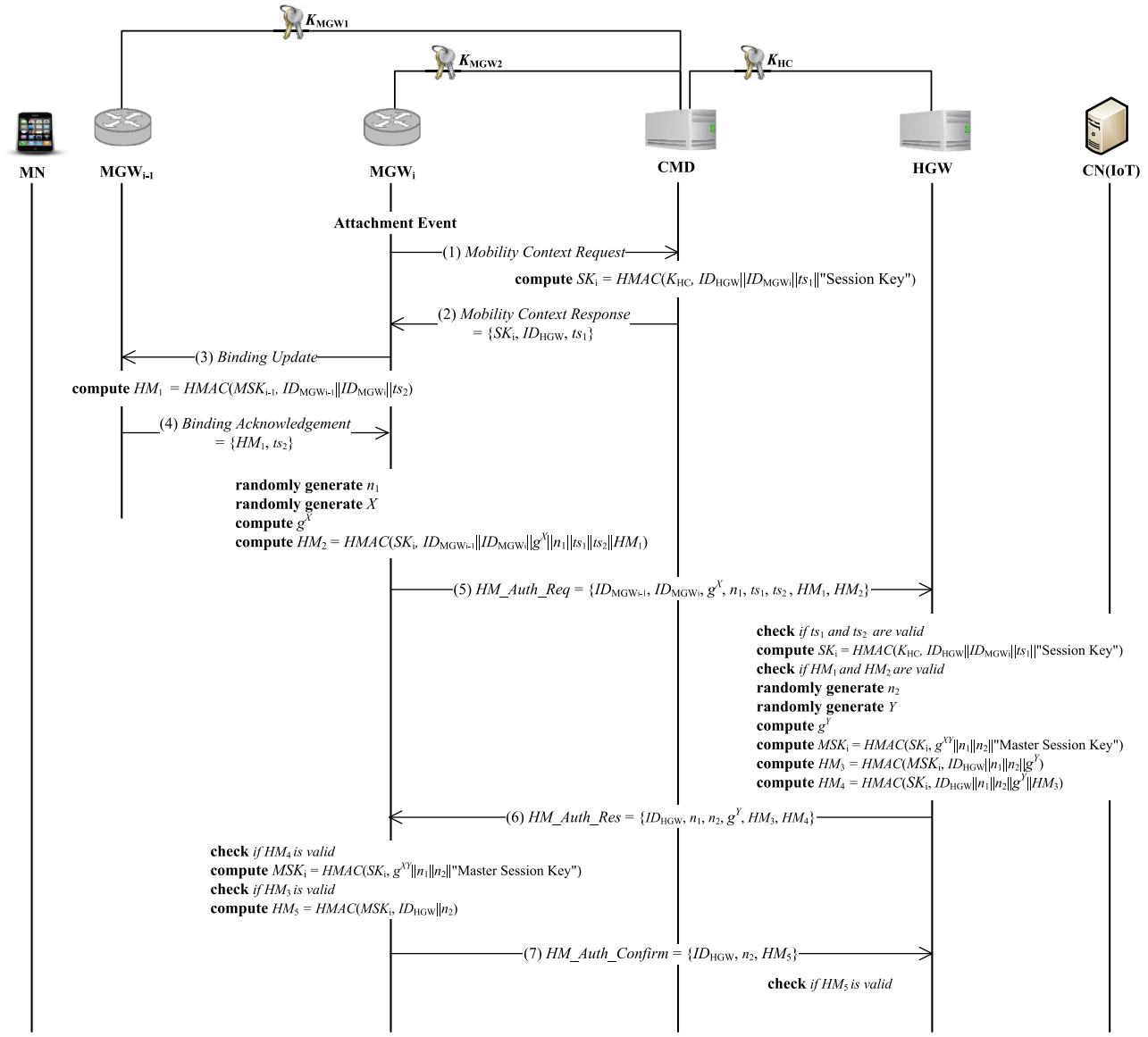


FIGURE 3. Route Optimization Handover Phase (RO-HO).

4) The valid HM_3 allows MGW_1 to safely perform the expensive public key computations for Diffie-Hellman key exchange without being vulnerable to the resource exhaustion attack. Thus, MGW_1 proceeds to calculate its private and public keys Y and g^Y, and in turn makes n_4 and g^{XY}, from which the master session key MSK_1 is then derived. Finally, the two HMAC values HM_4 and HM_5 are computed to compose and send the *HM_Auth_Req* message. Here, the former confirms the MGW_1's ownership of the master session key MSK_1 and the latter helps HGW to perform the Diffie-Hellman key exchange without being vulnerable to the resource exhaustion attack. As soon as receiving the *HM_Auth_Req* message, HGW attempts to verify the included HM_5, whose successful result enables HGW to securely get the master session key MSK_1 by computing $HMAC(K_{RO}, g^{XY}||n_3||n_4||$ "Master Session Key") as mentioned above. If such a verification is successful and thus MSK_1 is obtained, HGW tries to confirm that MGW_1 owns MSK_1 by validating HM_4 with it. In the case that both the two HMACs are valid, HGW can believe the MGW_1's ownership of MSK_1, and successfully authenticate MGW_1.

5) HGW concludes this phase by responding with the *HM_Auth_Confim* message that contains ID_{HGW}, n_4 and HM_6 to MGW_1. The inclusion of n_4 and HM_6 allows MGW_1 to validate that the last message is fresh and assure that the key exchange has been securely and successfully performed respectively. In more detail, MGW_1 finally confirms that HGW has MSK_1,

and thus is ready for the secure route optimization. As the final step, HGW and MGW_1 completely delete their Diffie-Hellman key pairs that were used to generate MSK_1 to support the perfect forward secrecy (PFS).

B. ROUTE OPTIMIZATION HANDOVER PHASE (RO_HO)

A secure route optimization must be continuously supported whenever an MN transfers from one MGW to another. For this reason, the Route Optimization Handover (RO_HO) phase, as shown in Figure 3, is designed. In this phase, the new MGW, to which the MN moves, securely gets the session key from its CMD, and then depends on that key to perform the mutual authentication and key exchange with the MN's HGW.

This phase is described in detail as follows:

1) If an attachment event with MN occurs, MGW_i transmits the *Mobility Context Request* message including the ID and address of the previous MGW_{i-1} to CMD in correspondent to the DMM protocol.
2) Upon receiving this request, CMD updates the network connection status of MN by setting the serving MGW record, associated to MN, to the ID and address of the new MWG_i. It also generates the current timestamp ts_1 and derives the session key SK_i through $HMAC(K_{HC}, ID_{HGW}||\ ID_{MGWi}||ts_1||$ "Session Key"). Then, it responds with the *Mobility Context Response message* including SK_i, ID_{HGW}, and ts_1 to MGW_i.
3) Before handling MN's handover, MGW_i uses the *Binding Update* message to request the binding update and tunneling for the transmission of MN data traffic to MGW_{i-1}.
4) In order to continually support the route optimization with HGW, MGW_{i-1} generates the current timestamp ts_2 and calculates the HMAC value $HM_1 = HMAC(MSK_{i-1}, ID_{MGWi-1}||\ ID_{MGWi}||ts_2)$ instead of preparing for the requested tunneling. Then, the *Binding Acknowledgement* message including these two values is transmitted to MGW_i. On arrival of this message, MGW_i first checks if the included timestamp ts_2 is fresh and the included HM_1 is valid. In positive case, it can be sure that the requested binding update is successfully performed as well as the route optimization should be continually supported.
5) If HM_1 is valid, MGW_i generates the random nonce n_1 and the Diffie-Hellman public key pair X and g^X, followed by computing HM_2 with the session key SK_i given by CMD in the *Mobility Context Response* message. Then, the *HM_Auth_Req* message is composed and transmitted to HGW. At this point, it is worth to note that this message includes the two HMAC values HM_1 and HM_2 where HM_1 shows that MGW_{i-1} confirms the MN's handover and HM_2 shows that MGW_i intends to continue the route optimization with HGW. Once the *HM_Auth_Req* message is received, HGW verifies that the two timestamps ts_1 and ts_2 are valid and computes SK_i, then validating HM_1 and HM_2 by using MSK_{i-1} and SK_i respectively. As mentioned above, if the timestamps and the HMAC values are correct, HGW can trust that the previous and new MGWs agree with the MN's handover and the route optimization needs to be continued. That makes it possible for HGW to prevent a malicious MGW from deceiving itself into redirecting the MN's data traffic. Moreover, with the help of HM_2, HGW can defend against the reply, man-in-the middle, and resource exhaustion attacks.
6) If the *HM_Auth_Req* message is valid, MGW_i generates the random nonce n_2 and its own Diffie-Hellman public key pair Y and g^Y, followed by deriving the ith master session key MSK_i through $HMAC(SK_i, g^{XY}||n_1||n_2||$ "Master Session Key"). At this point, HGW can count on HM_2 to prevent the man-in-the middle and resource exhaustion attacks caused by the Diffie-Hellman key exchange. Afterwards,MSK_i and SK_i are utilized to compute the two HMAC values HM_3 and HM_4. The first value confirms that HGW has MSK_i while the second value allows MGW_{i-1} to safely performs the expensive public key operations. Finally, HGW sends MGW_i the *HM_Auth_Res* message. Upon receipt of the *HM_Auth_Res* message, MGW_i checks if the received n_1 is same as the original one that it sent and validates HM_4 with SK_i. If correct, it performs the Diffie-Hellman key exchange to get MSK_i, which is then used to verify HM_3. In the case that HM_3 is valid, MGW_i can authenticate HGW while confirming that HGW owns MSK_i.
7) MGW_i concludes the handover process by sending HGW the *HM_Auth_Confirm* message protected by HM_5. On receiving this message, HGW verifies if the included n_2 is equal to the original one sent by itself and HM_5 is correct. If this verification is successful, MGW_i can be authenticated to HGW, which thus confirms the MGW_i's ownership of MSK_i. In order to support the perfect forward secrecy, the two parties remove their public key pair. As the result of this phase, MGW_i and HGW successfully performs the mutual authentication

TABLE 2. 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

TABLE 3. Rules of BAN logic.

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

and key exchange after the DMM based binding update procedure.

IV. FORMAL VERIFICATION

In this section, the proposed protocol is formally verified through BAN-logic [20], [34] and AVISPA [21]. These two verification methods could complement the weaknesses of each other, hence employing these tools provide a more extensive and robust verification of the proposed protocol.

A. FORMAL VERIFICATION WITH BAN-LOGIC

BAN-logic, presented by Burrows, Abadi, and Needham, has been one of the most popular formal security verification methods owing to its simplicity, intuitive, and robust [7], [35], [36]. Tables 2 and 3 show the notations and inference rules of BAN logic.

For a formal verification based on BAN-logic, a security protocol is first translated into an idealized version and its assumptions and goals are defined, followed by repeated applications of the inference rules until the intended beliefs are obtained.

1) RO-INIT PHASE

As the first step, the RO-INIT phase is idealized as follow.

(11) $HGW \rightarrow CMD : \{ID_{HGW}, I\ D_{MN}, n_1, t\ s_1, H\ M_1\}_{K_{BHC}}$
where $HM_1 = \langle ID_{HGW}, I\ D_{MN}, n_1, t\ s_1\rangle_{K_{HC}}$
(12) $CMD \rightarrow HGW : \langle ID_{CMD}, I\ D_{MGW_1}, n_1, n_2$
$MGW_1 \overset{K_RO}{\Longleftrightarrow} HGW, T_{HGW}\rangle_{K_{HC}}$
where $T_{HGW} = \{ID_{MN}, ID_{CMD}, T_{EXP}, MGW_1$
$\overset{K_{RO}}{\Longleftrightarrow} |GW\}_{K_{MGW_1}}$
(13) $HGW \rightarrow MGW_1 : [T_{HGW}, \langle ID_{HGW}, \overset{g^X}{\Longrightarrow} HGW, n_3, ts_2,$
$T_{HGW}, MGW_1 \overset{K_{RO}}{\rightarrow} HGW\rangle_{K_{RO}}]$
(14) $MGW_1 \rightarrow HGW : \langle ID_{MGW1}, n_3, n_4^g \rightarrow MGW_1, HM_4$
$MGW_1^{[N_{EO}]} \overset{NGW}{\oplus} HGW\rangle_{K_{RO}}$
where $HM_4\langle ID_{MGW1}, n_3, n_4 \overset{g^Y}{\rightarrow} MGW_1 MGW_1$
$\overset{MSK_1}{\Longleftrightarrow} HGW\rangle_{MSK_1}$
(15) $MGW_1 \rightarrow HGW : \langle ID_{HGW}, n_4, MGW_1 \overset{MSK_1}{\longrightarrow} HGW\rangle_{MSK_1}$

Based on the idealized form, the following assumptions are made.

(A1) CMD believes $CMD \overset{K_{EHC}}{\longleftrightarrow} HGW$
(A2) CMD believes $\#(ts_1)$
(A3) CMD believes $CMD \overset{K_{HC}}{\Longleftrightarrow} HGW$
(A4) HGW believes $CMD \overset{K_{HC}}{\Longleftrightarrow} HGW$
(A5) HGW believes $\#(n_1)$
(A6) HGW believes CMD controls $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$
(A7) MGW_1 believes $MGW_1 \overset{K_{MGW_1}}{\longleftrightarrow} CMD$
(A8) MGW_1 believes $\#(T_{EXP})$
(A9) MGW_1 believes CMD controls $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$
(A10) MGW_1 believes $\#(ts_2)$
(A11) MGW_1 believes $\overset{g^Y}{\longrightarrow} MGW_1$
(A12) MGW_1 believes $\#(n_4)$
(A13) HGW believes $\#(n_3)$
(A14) HGW believes $\overset{g^X}{\longrightarrow} HGW$

In addition, we define the 15 goals as shown below.

(G1) CMD *believes* HGW *believes* ID_{MN}
(G2) MGW_1 *believes* CMD *believes* ID_{MN}
(G3) CMD *believes* HGW *believes* ID_{HGW}
(G4) HGW *believes* CMD *believes* ID_{CMD}
(G5) HGW *believes* CMD *believes* T_{HGW}
(G6) MGW_1 *believes* HGW *believes* ID_{HGW}
(G7) HGW *believes* MGW_1 *believes* ID_{MGW1}
(G8) HGW *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$
(G9) HGW *believes* MGW_1 *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$
(G10) MGW_1 *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$
(G11) MGW_1 *believes* HGW *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$
(G12) MGW_1 *believes* $MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW$
(G13) MGW_1 *believes* HGW *believes* $MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW$
(G14) HGW *believes* $MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW$
(G15) HGW *believes* MGW_1 *believes* $MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW$

Here, (G1) and (G2) mean that the route optimization for the MN is accepted by CMD and MGW_1, and (G5) is the basis for HGW to continue the steps (3)-(5) with MGW_1. In addition, (G3) and (G4) show the successful mutual authentication between CMD and HGW while (G6) and (G7) show the successful mutual authentication between MGW_1 and HGW. Finally, (G8)-(G15) indicate that K_{RO} and MSK_1 are successfully exchanged between MGW_1 and HGW.

From (I1), we derive:

(D1)CMD *sees*$\{ID_{HGW}, ID_{MN}, n_1, ts_1, HM_1\}_{K_{EHC}}$
(D2) CMD *believes* HGW *believes* $[ID_{HGW}, ID_{MN}, n_1, ts_1, HM_1]$

by (D1), (A1), MM, (A2), FR, NV

(D3) CMD *believes* HGW *believes* ID_{MN}

by (D2), BC

(D4) CMD *believes* HGW *believes* HM_1

by (D2), BC

(D5) CMD *believes* HGW *said* $[ID_{HGW}, ID_{MN}, n_1, ts_1]$

by (D4), (A3), MM

(D6) CMD *believes* HGW *believes* $[ID_{HGW}, ID_{MN}, n_1, ts_1]$

by (D5), (A2), FR, NV

(D7) CMD *believes* HGW *believes* ID_{MN}

by (D6), BC

(D8) CMD *believes* HGW *believes* ID_{HGW}

by (D6), BC

From (I2), we derive:

(D9)HGW *sees* $\langle ID_{CMD}, ID_{MGW_1}, n_1, n_2, MGW_1 \overset{KGW}{\rightarrow} HGW, T_{HGW}\rangle_{K_{HC}}$

(D10) HGW *believes* CMD *believes* $[ID_{CMD}, ID_{MGW_1}, n_1, n_2, MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW, T_{HGW}]$

by (D9), (A4), MM, (A5), FR, NV

(D11) HGW *believes* CMD *believes* ID_{CMD}

by (D10), BC

(D12) HGW *believes* CMD *believes* T_{HGW}

by (D10), BC

(D13) HGW *believes* CMD *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$

by (D10), BC

(D14) HGW *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$

by (D13), (A6), JR

From (I3), we derive:

(D15) MGW_1 *sees*T_{HGW}

(D16) MGW_1 *believes* CMD *believes* $\left[ID_{MN}, ID_{CMD}, T_{EXP}, MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW\right]$

by (D15), (A7), MM, (A8), FR, NV

(D17) MGW_1 *believes* CMD *believes* ID_{MN}

by (D16), BC

(D18) MGW_1 *believes* CMD *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$

by (D16), BC

(D19) MGW_1 *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$

by (D18), (A9), JR

(D20)MGW_1*sees*$\langle ID_{\mathrm{HGW}} \overset{g^X}{\rightarrow} HGW, n_3, ts_2, T_{HGW}, MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW\rangle_{K_{RO}}$

(D21) MGW_1 *believes* HGW *said* $\left[ID_{HGW}, \overset{g^X}{\longrightarrow} HGW, n_3, ts_2, T_{HGW}, MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW\right]$

by (D20), (D19), MM

(D22) MGW_1 *believes* HGW *believes* $\left[ID_{HGW}, \overset{g^X}{\longrightarrow} HGW, n_3, ts_2, T_{HGW}, MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW\right]$

by (D21), (A10), FR, NV

(D23) MGW_1 *believes* HGW *believes* ID_{HGW}

by (D22), BC

(D24) MGW_1 *believes HGW believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$

by (D22), BC

(D25) MGW_1 *believes* $MGW_1 \overset{g^{XY}}{\Longleftrightarrow} HGW$

by (D21), BC, (A11), DH

(D26) MGW_1 *believes HGW believes* n_3

by (D22), BC

(D27) MGW_1 *believes* $MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW$

by (D25), (D26), (A12)

From (I4), we derive:

(D28)HGW *sees* $\langle ID_{MGW1}, n_3, n_4, \overset{g^Y}{\rightarrow} MGW_1, HM_4, MGW_1 \overset{K_RO}{\Longleftrightarrow} HGW\rangle_{K_{RO}}$

(D29) HGW *believes* MGW_1 *said*

$[ID_{MGW1}, n_3, n_4, \overset{g^Y}{\longrightarrow} MGW_1, HM_4, MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW]$

by (D28), (D14), MM

(D30) HGW *believes* MGW_1 *believes*

$[ID_{MGW1}, n_3, n_4, \overset{g^Y}{\longrightarrow} MGW_1, HM_4, MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW]$

by (D29), (A13), FR, NV

(D31) HGW *believes* MGW_1 *believes* ID_{MGW1}

by (D30), BC

(D32) HGW *believes* MGW_1 *believes* $MGW_1 \overset{K_{RO}}{\Longleftrightarrow} HGW$

by (D30), BC

(D33) HGW *believes* $MGW_1 \overset{g^{XY}}{\Longleftrightarrow} HGW$

by (D29), BC, (A14), DH

(D34) HGW *believes* MGW_1 *believes* n_4

by (D30), BC

(D35) HGW *believes* $MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW$

by (D33), (D34), (A13)

(D36)HGW *sees* HM_4

by (D29), BC

(D37) HGW *believes* MGW_1 *believes*

$[ID_{MGW_1}, n_3, n_4, \overset{g^Y}{\longrightarrow} MGW_1, MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW]$

by (D36), (D35), MM, (A13), FR, NV

(D38) HGW *believes* MGW_1 *believes* ID_{MGW_1}

by (D37), BC

(D39) HGW *believes* MGW_1 *believes* $MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW$

by (D37), BC

From (I5), we derive:

(D40)MGW_1 *sees*$\langle ID_{HGW}, n_4, MGW_1 \overset{MS\mathbb{F}_1}{\Longleftrightarrow} HGW\rangle_{MSK_1}$

(D41)MGW_1 *believes HGW believes* $[ID_{HGW}, n_4, MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW]$

by (D40), (D27), MM, (A12), FR, NV

(D42) MGW_1 *believes HGW believes* ID_{HGW}

by (D41), BC

(D43) MGW_1 *believes HGW believes* $MGW_1 \overset{MSK_1}{\Longleftrightarrow} HGW$

by (D41), BC

It is shown from the above derived beliefs (D1)-(D43) that the RO-INIT phase achieves the goals (G1)-(G15). Moreover, we can obtain the following lemmas.

Lemma 1: The RO-INIT phase provides mutual authentication.

Proof: The derived beliefs (D8) and (D11) show that CMD and HGW mutually authenticate each other. On the other hand, we can see from (D23) and (D31) that based on K_{RO}, MGW_1 and HGW mutually authenticate each other. These beliefs are strengthened by (D31) and (D38), which also show the mutual authentication between MGW_1 and HGW based on MSK_1. Because MSK_1 is negotiated based on the Diffie-Hellman key exchange, (D31) and (D38), without being just redundant, can guarantee that the mutual authentication is strong enough for the route optimization. As a result, it is concluded that the RO-INIT phase achieves mutual authentication. □

Lemma 2: The session keys K_{RO} and MSK_1 are successfully exchanged between MGW_1 and HGW.

Proof: HGW is based on (D14) and (D35) to believe that the session keys K_{RO} and MSK_1 are securely exchanged between itself and MGW_1. Such a belief is enhanced and completed through (D32) and (D39), which indicates that HGW believes the correspondent's belief on the keys. Similarly, it is sure from (D19), (D24), (D27), and (D43), *i.e.*, the MGW_1's direct and indirect beliefs on K_{RO} and MSK_1, that it securely negotiates the keys with HGW. Therefore, we can show that the session keys K_{RO} and MSK_1 are successfully exchanged between MGW_1 and HGW. □

Lemma 3: The RO-INIT phase provides the perfect forward secrecy.

Proof: It can be seen from (D25) and (D33) that MGW_1 negotiates g^{XY} with MGW_1 by employing the Diffie-Hellman key exchange protocol. After this key agreement, the two parties remove their private key so that g^{XY} cannot be recovered even though some or all of the secret keys K_{HC}, K_{EHC}, and K_{RO} are exposed. Hence, we can say that g^{XY} and MSK_1, which is derived from g^{XY}, are protected with the perfect forward secrecy. As a result, it is concluded that the

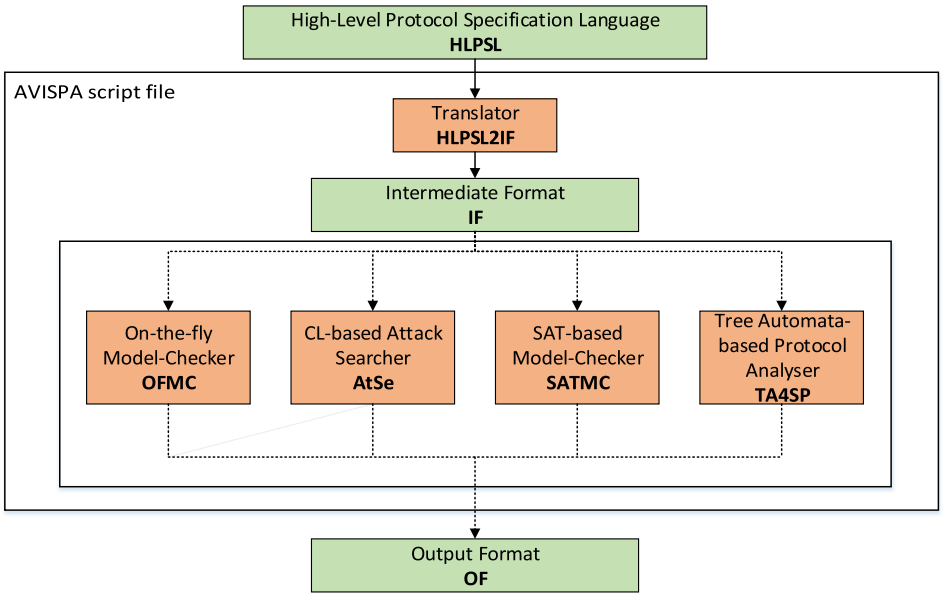


FIGURE 4. AVISPA Architecture.

RO-INIT phase achieves the perfect forward secrecy because the route optimization is secured based on MSK_1 after that phase. □

Lemma 4: The RO-INIT phase preserves MN's privacy.

Proof: In order to obtain (D3), the CMD's belief on ID_{MN}, the message meaning rule is first applied to the encrypted message $\{ID_{\mathrm{HGW}}, ID_{\mathrm{MN}}, n_1, ts_1, HM_1\}K_{\mathrm{EHC}}$. Thus, this belief indicates that ID_{MN} is known to CMD without being exposed. On the other hand, the MGW_1's belief (D17) is gained from T_{HGW}, which is encrypted with $K\mathrm{MGW}_1$. Similar to (D3), it thus shows that ID_{MN} is securely transmitted to MGW_1. As a result, during the RO-INIT phase, no external entity knows the MN's identifier ID_{MN}. That makes it possible to conclude that MN's privacy is preserved in this phase. □

Lemma 5: The RO-INIT phase defends against resource exhaustion attack.

Proof: According to (D10) and (D30), HGW successfully verifies HM_2 and HM_5 so that it can generate its own public key pair X and g^X as well as perform the Diffie-Hellman key agreement without being vulnerable to resource exhaustion attack. In the same way, MGW_1 first verifies the ticket T_{HGW}, and then performs the public key operations, thereby preventing resource exhaustion attack. From (D16), it is demonstrated that such a verification is successfully performed. Consequently, we can show that the RO-INIT phase defends against resource exhaustion attack. □

Lemma 6: The RO-INIT phase defends against malicious MGW.

Proof: In order to be successfully involved in the RO-INIT phase, MGW_1 should be first contacted by HGW, receive T_{HGW}, and show that it knows K_{RO}. Because this phase just initializes the route optimization between HGW and its intended MGW_1, it is impossible for a malicious MGW to redirect MN's traffic by deceiving HGW. (D16) shows that the ticket T_{HGW} can be decrypted and verified by only the intended MGW_1 having $K\mathrm{MGW}_1$. Moreover, (D19) shows that the intended MGW_1 obtains K_{RO}. Note that even though MGW_1 is malicious, it is limited to freely lunch attacks at its will. Accordingly, we can conclude that the RO-INIT phase defends against malicious MGW. □

Lemma 7: The RO-INIT phase provides confidentiality and integrity.

Proof: Confidentiality indicates that session keys are effectively exchanged between involved entities without any leakage as well as ID_{MN} is not exposed (i.e., privacy is kept). It has been shown in Lemma 2 that session keys K_{RO} and MSK_1 are securely exchanged and can be enhanced through Lemma 3 in a way that perfect forward secrecy is guaranteed by the deletion of the private key used in the Diffie-Hellman key exchange protocol. Moreover, the privacy can be supported through Lemma 4 in which no external entity can know the MN's identifier ID_{MN}. On the other hand, integrity indicates that the HMAC values HM1– HM6 are valid. It can be shown from the obtained beliefs (D4), (D10), (D22), D(30), D(36) and D(41) that the value of all HMACs are correct, which subsequently proves support to the integrity requirement. Accordingly, we can conclude that the RO-INIT phase provides confidentiality and integrity. □

2) RO-HO PHASE

The formal verification for the RO-HO phase is started by idealizing and defining the assumptions as shown below.

(H1) $MGW_i \rightarrow HGW : \langle ID_{MGW_{i-1}}, ID_{MGW_i}, \xrightarrow{g^X} MGW_i, n_1, ts_1, ts_2 HM_1 \rangle_{SK_i}$
where $HM_1 = \langle ID_{MGW_{i-1},}, ID_{MGW_i}, ts_2 \rangle_{MSK_{i-1}}$

(H2) $HGW \rightarrow MGW_i : \langle ID_{HGW}, n_1, n_2, \xrightarrow{g^Y} HGW, HM_3 \rangle_{SK_i}$
where $HM_3 = \langle ID_{HGW}, n_1, n_2, \xrightarrow{g^Y} HGW, MGW_i^{NSK_i} HGW \rangle_{MSK_i}$

(H3) $MGW_i \rightarrow HGW : \langle ID_{MGW_i}, n_2, MGW_i^{MSK_i} HGW \rangle_{MSK_i}$

(A15) HGW *believes* $MGW_i \overset{SK_i}{\Longleftrightarrow} HGW$

(A16) HGW *believes* $\#(ts_2)$

(A17) HGW *believes* $\xrightarrow{g^Y} HGW$

(A18) HGW *believes* $\#(n_2)$

(A19) HGW *believes* $MGW_{i-1} \overset{MSK_{i-1}}{\Longleftrightarrow} HGW$

(A20) MGW_i *believes* $MGW_i \overset{SK_i}{\Longleftrightarrow} HGW$

(A21) MGW_i *believes* $\#(n_1)$

(A22) MGW_i *believes* $\xrightarrow{g^X} MGW_i$

In addition, the following goals are set where (G16)-(G17) indicate the mutual authentication between MGW_i and HGW, (G18)-(G21) mean the session key MSK_i exchange between MGW_i and HGW, and (G22)-(G23) express HGW's belief on the involved MGWs' agreement on MN's handover. Note that (G22)-(G23) are specially added to formally verify if the RO-HO phase can prevent a legitimate but malicious MGW's attack by counting on HM_1 and HM_2.

(G16) HGW *believes* MGW_i *believes* ID_{MGW_i}

(G17) MGW_i *believes* HGW *believes* ID_{HGW}

(G18) HGW *believes* $MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW$

(G19) MGW_i *believes* $MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW$

(G20) MGW_i *believes* HGW *believes* $MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW$

(G21) HGW *believes* MGW_i *believes* $MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW$

(G22) HGW *believes* MGW_i *believes* $\left[ID_{MGW_{i-1}}, ID_{MGW_i}\right]$

(G23) HGW *believes* MGW_{i-1} *believes* $\left[ID_{MGW_{i-1}}, ID_{MGW_i}\right]$

From (H1), we derive:

(D44) HGW *sees* $\langle ID_{MGW'_{i-1}}, ID_{MGW'_i} \xrightarrow{g^X} MGW_i, n_1, ts_1, ts_2, HM_1 \rangle_{SK_i}$

(D45) HGW *believes* MGW_i *said*
$\left[ID_{MGW_{i-1}}, ID_{MGW_i}, \xrightarrow{g^X} MGW_i, n_1, ts_1, ts_2, HM_1\right]$
by (D44), (A15), MM

(D46) HGW *believes* MGW_i *believes*
$\left[ID_{MGW_{i-1}}, ID_{MGW_i}, \xrightarrow{g^X} MGW_i, n_1, ts_1, ts_2, HM_1\right]$
by (D45), (A16), FR, NV

(D47) HGW *believes* MGW_i *believes* $\left[ID_{MGW_{i-1}}, ID_{MGW_i}\right]$
by (D46), BC

(D48) HGW *believes* MGW_i *believes* n_1
by (D46), BC

(D49) HGW *believes* MGW_i *said* $\xrightarrow{g^X} MGW_i$
by (D45), BC

(D50) HGW *believes* $MGW_i \overset{g^{XY}}{\Longleftrightarrow} HGW$
by (D49), (A17), DH

(D51) HGW *believes* $MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW$
by (D50), (D48), (A18)

(D52) HGW *sees* HM_1
by (D45), BC

(D53) HGW *believes* MGW_{i-1} *believes* $\left[ID_{MGW_{i-1}}, ID_{MGW_i}\right]$
by (D52), (A19), MM, (A16), FR, NV, BC

From (H2), we derive:

(D54) $MGW_i sees \left\langle ID_{HGW}, n_1, n_2, \xrightarrow{g^Y} HGW, HM_3 \right\rangle_{SK_i}$

(D55) MGW_i *believes* HGW *said*
$\left[ID_{HGW}, n_1, n_2, \xrightarrow{g^Y} HGW, HM_3\right]$
by (D54), (A20), MM

(D56) MGW_i *believes* HGW *believes*
$\left[ID_{HGW}, n_1, n_2, \xrightarrow{g^Y} HGW, HM_3\right]$
by (D53), (A21), FR, NV

(D57) MGW_i *believes* HGW *believes* ID_{HGW}
by (D56), BC

(D58) MGW_i *believes* HGW *believes* n_2
by (D56), BC

(D59) MGW_i *believes* HGW *said* $\xrightarrow{g^Y} HGW$
by (D55), BC

(D60) MGW_i *believes* $MGW_i \overset{g^{XY}}{\Longleftrightarrow} HGW$
by (D59), (A22), DH

```
role role_HGW(
HGW, CMD, MGW                                  : agent,
IDhgw, IDmn, G                                 : text,
Khc, Kehc                                      : symmetric_key,
HMAC                                           : hash_func,
SND_HC, RCV_CH, SND_HM, RCV_MH : channel(dy)
)played_by HGW
def=

local
        State                                  : nat,

        N1, Ts1, IDcmd, IDmgw1,
        N2, N3, X, Ts2, N4                     : text,
        HM1, EMsg1, Thgw, Kro,
        GX, HM3, GY, GXY, MSK1, HM6            : message

init
        State := 0

transition
1. State = 0   /\ RCV_CH(start)=|>
   State' := 2 /\ N1' := new()
               /\ Ts1' := new()
               /\ HM1' := HMAC(Khc.IDhgw.IDmn.N1'.Ts1')
               /\ EMsg1' := {IDhgw.IDmn.N1'.Ts1'.HM1'}_Kehc
               /\ SND_HC(IDhgw.EMsg1')
               /\ secret(Khc, sec1, {HGW, CMD})
               /\ witness(HGW, CMD, auth1, Khc)


3. State = 2   /\ RCV_CH(IDcmd'.IDmgw1'.N1.N2'.Thgw'.
                  HMAC(Khc.IDcmd'.IDmgw1'.IDmn.N1.N2'.Thgw'))=|>
   State' := 4 /\ Kro' := HMAC(Khc.N1.N2)
               /\ N3' := new()
               /\ X' := new()
               /\ GX' := exp(G,X')
               /\ Ts2' := new()
               /\ HM3' := HMAC(Kro'.IDhgw.IDcmd'.
                                  IDmn.N3'.GX'.Ts2'.Thgw')
               /\ SND_HM(IDhgw.GX'.N3'.Ts2'.Thgw'.HM3')
               /\ request(HGW, CMD, auth2, N2')
               /\ witness(HGW, MGW, auth3, N3')

5. State = 4
               /\ RCV_MH(IDmgw1'.GY'.N3.N4'.
                     HMAC(HMAC(Kro.GXY'.N3.N4').
                        IDmgw1'.N3.N4'.GY').
                        HMAC(Kro.IDmgw1'.N3.N4'.GY'.
                           HMAC(MSK1'.IDmgw1'.
                           N3.N4'.GY'))) =|>
   State' := 6 /\ GXY' := exp(GY,X)
               /\ MSK1' := HMAC(Kro.GXY'.N3.N4')
               /\ HM6' := HMAC(MSK1'.IDhgw.N4')
               /\ SND_HM(IDhgw.N4'.HM6')
               /\ request(HGW, MGW, auth4, N4')

end role
```

FIGURE 5. HGW's Basic Role for the RO-INIT phase.

```
role role_CMD(
HGW, CMD, MGW                                  : agent,
IDcmd, IDmgw1                                  : text,
Khc, Kmgw1, Kehc                               : symmetric_key,
HMAC                                           : hash_func,
SND_CH, RCV_HC                                 : channel(dy)
)played_by CMD
def=

local
        State                                  : nat,
        IDhgw, IDmn, N1, Ts1, N2,
        Texp                                   : text,
        Kro, Thgw, HM2                         : message

init
State := 1

transition
2. State = 1   /\ RCV_HC(IDhgw'.{IDhgw'.IDmn'.N1'.Ts1'.
                     HMAC(Khc.IDhgw'.IDmn'.N1'.Ts1')}_Kehc)=|>
   State' := 3 /\ N2' := new()
               /\ Kro' := HMAC(Khc.N1.N2')
               /\ Texp' := new()
               /\ IDcmd' := new()
               /\ Thgw' := {IDmn'.IDcmd.Texp'.Kro'}_Kmgw1
               /\ HM2' := HMAC(Khc.IDcmd.IDmgw1.
                                  IDmn'.N1'.N2',Thgw')
               /\ SND_CH(IDcmd.IDmgw1.N1'.N2'.Thgw'.HM2')
               /\ secret(Kmgw1, sec2, {CMD, MGW})
               /\ request(CMD, HGW, auth1, Khc)
               /\ witness(CMD, HGW, auth2, N2')

end role
```

FIGURE 6. CMD's Basic Role for the RO-INIT phase.

(D61) MGW_i *believes* $MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW$

by (D60), (D58), (A21)

(D62) $MGW_i sees HM_3$

by (D55), BC

(D63) MGW_i *believes HGW believes*

$$\left[ID_{HGW}, n_1, n_2, \xrightarrow{g^Y} HGW, MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW\right]$$

by (D62), (D61), MM, (A21), FR, NV

(D64) MGW_i *believes HGW believes* ID_{HGW}

by (D63), BC

(D65) MGW_i *believes HGW believes* $MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW$

by (D63), BC

From (H3), we derive:

(D66) HGW *sees* $\left\langle ID_{MGW_i}, n_3, MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW\right\rangle_{MSK_i}$

(D67) HGW *believes* MGW_i*believes* $[ID_{MGW_i}, n_2, MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW]$

by (D66), (D51), MM, (A18), FR, NV

(D68) HGW *believes* MGW_i *believes* ID_{MGW_i}

by (D67), BC

(D69) HGW *believes* MGW_i *believes* $MGW_i \overset{MSK_i}{\Longleftrightarrow} HGW$

by (D67), BC

Consequently, the above verification shows that the RO-HO phase can fulfil the goals (G16)-(G23). Moreover, we can derive the following lemmas from (D44)-(D69).

Lemma 8: The RO-HO phase provides mutual authentication.

Proof: The obtained beliefs (D48), (D57), (D64), and (D68) show that MGW_i and HGW mutually authenticate each other. Note that (D48) and (D57) are derived based on SK_i while (D64), and (D68) are derived based on MSK_i. That is, the former is enhanced by the latter because MSK_i is strongly negotiated through the Diffie-Hellman key exchange protocol. Consequently, we can conclude that the RO-HO phase provides mutual authentication. □

Lemma 9: The session key MSK_i is successfully exchanged between MGW_i and HGW.

Proof: According to (D51) and (D61), MGW_i and HGW believe that MSK_1 is successfully negotiated

```
role role_MGW(
HGW, CMD, MGW                                   : agent,
IDmn, G, IDmgw1                                 : text,
Kmgw1                                           : symmetric_key,
HMAC                                            : hash_func,
SND_MH, RCV_HM                                  : channel(dy)
)played_by MGW
def=

local
        State                                   : nat,
        IDhgw, IDcmd, N3, Ts2, N4, Y,Texp       : text,
        GX, Kro, GY, GXY,
        MSK1, HM4, HM5                          : message

init
        State := 3

transition
4. State = 3            /\ RCV_HM(IDhgw'.GX'.N3'.Ts2'.
                                {IDmn.IDcmd'.Texp'.Kro'}_Kmgw1.
                                 HMAC(Kro'.IDhgw'.IDcmd'.IDmn.N3'.GX'.Ts2'.
                                      {IDmn.IDcmd'.Texp'.Kro'}_Kmgw1)) =|>
   State' := 5          /\ N4' := new()
                        /\ Y' := new()
                        /\ GY' := exp(G,Y')
                        /\ GXY' := exp(GX',Y')
                        /\ MSK1' := HMAC(Kro'.GXY'.N3'.N4')
                        /\ HM4' := HMAC(MSK1'.IDmgw1.N3'.N4'.GY')
                        /\ HM5' := HMAC(Kro'.IDmgw1.N3'.N4'.GY'.HM4')
                        /\ SND_MH(IDmgw1.GY'.N3'.N4'.HM4'.HM5')
                        /\ request(MGW, HGW, auth3, N3')
                        /\ witness(MGW, HGW, auth4, N4')

6. State = 5            /\ RCV_HM(IDhgw.N4.HMAC(MSK1.IDhgw.N4)) =|>

   State' := 7

end role
```

FIGURE 7. MGW's Basic Role for in the RO-INIT phase.

```
role role_CMD(
MGW1, MGW2, CMD, HGW : agent,
IDmgw2, IDhgw : text,
Kmgw1, Kmgw2, Khc : symmetric_key,
HMAC : function,
SND_CM2, RCV_M2C : channel(dy)
)played_by CMD
def=

local
State : nat,
Mobility_Context_Req : text,
Ts1 : text,
SKi : message

init
State := 1

transition
2. State = 1        /\ RCV_M2C(Mobility_Context_Req') =|>
   State' := 3      /\ Ts1' := new()
                    /\ SKi' := HMAC(Khc.IDhgw.IDmgw2.Ts1')
                    /\ SND_CM2({SKi'.IDhgw.Ts1'}_Kmgw2)

end role
```

FIGURE 8. CMD's Basic Role for in the RO-HO phase.

between themselves. Such a belief is evolved through the indirect belief that each party believes its correspondent's belief on MSK_1. That makes it possible to prove that MSK_1 are successfully exchanged between MGW_i and HGW. □

Lemma 10: The RO-HO phase provides the perfect forward secrecy.

Proof: (D50) and (D60) show that g^{XY} is established between MGW_i and HGW through the Diffie-Hellman key exchange protocol. Note that the private keys X and Y are immediately removed from the two parties to prevent g^{XY} from being recovered in any case. Accordingly, we can

```
role role_MGW_1(
MGW1, MGW2, CMD, HGW : agent,
IDmgw1, IDmgw2, MSK1 : text,
HMAC : function,
SND_M1M2, RCV_M2M1 : channel(dy)
)played_by MGW1
def=

local
State : nat,
Binding_Update : text,

Ts2 : text,
HM1 : message

init
State := 3

transition
4. State = 3        /\ RCV_M2M1(Binding_Update') =|>
   State' := 5      /\ Ts2' := new()
                    /\ HM1' := HMAC(MSK1.IDmgw1.IDmgw2.Ts2')
                    /\ SND_M1M2(Ts2'.HM1')
                    /\ secret(MSK1, sec3, {MGW1, HGW})

end role
```

FIGURE 9. Previous MGW's Basic Role in the RO-HO phase.

conclude that MSK_i derived from g^{XY} is protected with the perfect forward secrecy. Consequently, it is demonstrated that the RO-HO phase provides the perfect forward secrecy because MSK_i is utilized to protect the route optimization. □

Lemma 11: The RO-HO phase preserves MN's privacy.

Proof: During the RO-HO phase, MN's identifier ID_{MN} is not used and exposed. Therefore, we can say that the RO-HO phase preserves MN's privacy. □

Lemma 12: The RO-HO phase defends against resource exhaustion attack.

Proof: Similar to the RO-INIT phase, this phase prevents the resource exhaustion attack by ensuring that MGW_i and HGW perform the Diffie-Hellman key agreement only if the relevant HMAC value is valid. Details are as follows. During the binding update procedure, MGW_i needs to check if ts_2 is within its time window. Only if the timestamp is fresh, MGW_i prepares for the next message while generating its its public key pair. In addition, based on (D46) showing HM_2 is valid, HGW can safely perform the required public key operations. At last, according to (D56), while trusting HM_2, MGW_i performs the key agreement, thus not being vulnerable to the resource exhaustion attack. From the above, we can conclude that the RO-HO phase defends against resource exhaustion attack. □

Lemma 13: The RO-HO phase defends against malicious MGW.

Proof: In this phase, HGW verifies both the two HMAC values HM_1 and HM_2, which are computed by MGW_{i-1} and MGW_i respectively. In other words, this phase can be advanced after confirming that the two involved MGW agree MN's handover. Such agreement, shown through (D47) and (D53), can prevent a malicious MGW from freely attempting at its will to trick HGW into redirecting MN's traffic at its will. As a result, we can conclude that the RO-HO phase defends against malicious MGW. □

```
role role_HGW(
MGW1, MGW2, CMD, HGW : agent,
G, MSK1, IDhgw : text,
Khc : symmetric_key,
HMAC : function,
SND_HM2, RCV_M2H : channel(dy)
)played_by HGW
def=

local
State : nat,
IDmgw1, IDmgw2, N1, Ts1, Ts2, N2, Y : text,
SKi,HM1,HM2,GY,HM3,HM4,MSK2,HM5,GX,GXY :message

init
State := 5

transition
6. State = 5 /\ RCV_M2H(IDmgw1'.IDmgw2'.GX'.N1'.Ts1'.Ts2'.
HMAC(MSK1.IDmgw1'.IDmgw2'.Ts2').HMAC(SKi'.IDmgw1'.IDmgw2'.
GX'.N1'.Ts1'.Ts2'.HMAC(MSK1.IDmgw1'.IDmgw2'.Ts2'))) =|>
      State' := 7 /\ SKi' := HMAC(Khc.IDhgw.IDmgw2'.Ts1')
      /\ N2' := new()
      /\ Y' := new()
      /\ GY' := exp(G,Y')
      /\ GXY' := exp(GX', Y')
      /\ MSK2' := HMAC(SKi'.GXY'.N1'.N2')
      /\ HM3' := HMAC(MSK2'.IDhgw.N1'.N2'.GY')
      /\ HM4' := HMAC(SKi'.IDhgw.N1'.N2'.GY'.HM3')
      /\ SND_HM2(IDhgw.N1'.N2'.GY'.HM3'.HM4')
      /\ wrequest(HGW,MGW2,auth1,SKi')
      /\ witness(HGW,MGW2,auth2,N2')
      /\ secret(MSK2',sec2,{HGW,MGW2})

8. State = 7 /\ RCV_M2H(IDhgw.N2.HMAC(MSK2.IDhgw.N2)) =|>
      State' := 9

end role
```

FIGURE 10. HGW's Basic Role in the RO-HO phase.

Lemma 14: The RO-HO phase provides confidentiality and integrity.

Proof: Confidentiality indicates that session key is effectively exchanged between involved entities without any leakage. It has been shown in Lemma 9 that session key MSK_i is securely exchanged and can be enhanced through Lemma 10 in a way that perfect forward secrecy is guaranteed by the deletion of private key use in the Diffie-Hellman key exchange protocol. On the other hand, integrity indicates that HMAC values HM1 – HM5 are valid. It can be shown from the obtained beliefs (D46), (D52), (D56), (D63), and (D67) that the value of all HMACs are correct, which subsequently proves support to the integrity requirement. Accordingly, we can conclude that the RO-HO phase provides confidentiality and integrity. □

B. FORMAL VERIFICATION WITH AVISPA

Here, a formal verification is performed on the proposed security protocol through a security analysis automation tool known as Automated Validation of Internet Security Protocols and Applications (AVISPA) [7]. AVISPA is utilized to specify security protocols, along with the desired security properties, to analyze their flaws. For AVISPA based verification, a protocol first needs to be modelled in High-Level Protocol Specification Language (HLPSL), which is an AVISPA role-based language. Then, the HLPSL model is automatically converted to an intermediate format (IF) using HLPSL2IF translator, as shown in Figure 4. The converted

```
role role_CMD(
MGW1, MGW2, CMD, HGW : agent,
IDmgw2, IDhgw : text,
Kmgw1, Kmgw2, Khc : symmetric_key,
HMAC : function,
SND_CM2, RCV_M2C : channel(dy)
)played_by CMD
def=

local
State : nat,
Mobility_Context_Req : text,
Ts1 : text,
SKi : message

init
State := 1

transition
2. State = 1          /\ RCV_M2C(Mobility_Context_Req') =|>
   State' := 3        /\ Ts1' := new()
                      /\ SKi' := HMAC(Khc.IDhgw.IDmgw2.Ts1')
                      /\ SND_CM2({SKi'.IDhgw.Ts1'}_Kmgw2)

end role
```

FIGURE 11. CMD's Basic Role for in the RO-HO phase.

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/DMM_RO.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.02s
 visitedNodes: 4 nodes
 depth: 3 plies
```

FIGURE 12. Verification Result on the RO-INIT Phase by OFMC.

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

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

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed  : 10 states
 Reachable  : 3 states
 Translation: 0.02 seconds
 Computation: 0.00 seconds
```

FIGURE 13. Verification Result on the RO-INIT Phase by AtSe.

IF version is in turn thoroughly analyzed by the backend modules, *i.e,* to the On-the-fly Model-Checker (OFMC), CL-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC), and Tree-Automata-based Protocol Analyzer (TA4SP).

1) HLSPL MODEL

As the first step, the RO-INIT and RO-HO phases are translated into the HLSPL models. The former's basic roles, role_HGW, role_CMD, and role_MGW, are shown

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/DMM_RO_2.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.11s
  visitedNodes: 56 nodes
  depth: 7 plies
```

FIGURE 14. Verification Result on the RO-HO Phase by OFMC.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/DMM_RO_2.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed  : 24 states
  Reachable  : 18 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

FIGURE 15. Verification Result on the RO-HO Phase by AtSe.

in Figures 5, 6, and 7 while the latter's basic roles, role_MGW_2, role_MGW_1, role_HGW, and role_CMD, are depicted in Figures 8, 9, 10, and 11. Here, role_MGW_2 and role_MGW_1 model the new and previous MGWs respectively.

2) VERIFICATION RESULT

Figures 12, 13, 14, and 15 show the formal verification results gained by running the two backend modules OFMC and AtSe for the RO-INIT and RO-HO phases. The simulation diagrams for the two phases are also depicted in Figures 16 and 17. According to the verification results, both the RO-INIT and RO-HO phases of the protocol are safe against known attacks.

TABLE 4. The comparison of the proposed protocol and other standard security protocols in terms of security properties.

Scheme	Security Features							
	ⓐ	ⓑ	ⓒ	ⓓ	ⓔ	ⓕ	ⓖ	ⓗ
EAP-TLS	✓	✓	✓	✓	×	×	×	×
EAP-AKA	✓	✓	✓	✓	×	×	✓	×
EAP-IKEv2	✓	✓	✓	✓	×	✓	×	×
DMM-RO	✓	✓	✓	✓	✓	✓	✓	✓

Note:

✓: Support, ×: Not Support,

ⓐ: Confidentiality ⓑ: Integrity ⓒ: Mutual Authentication

ⓓ: Key Exchange ⓔ: Privacy ⓕ: Perfect Forward Secrecy

ⓖ: Defence against Resource Exhaustion Attack

ⓗ: Defence against Attack by Malicious MGWs

V. COMPARISON ANALYSIS

In this section, the proposed protocol is compared with the widely used standard security protocols EAP-TLS [30], EAP-AKA [31], and EAP-IKEv2 [32] that can be applied to protect the route optimization between MGW and HGW.

Table 4 gives a comparative analysis among the proposed protocol and other three security standards based on security properties. From this analysis, we can see that EAP-TLS, EAP-AKA, and EAP-IKEv2 don't support privacy while not preventing attacks by malicious MGWs. Additionally, EAP- TLS and EAP-AKA don't support perfect forward secrecy while EAP-TLS and EAP-IKEv2 are susceptible to resource exhaustion attacks. Accordingly, it can be concluded that the proposed protocol offers better security than others. On the other hand, the proposed protocol is compared with other standard security protocols in terms of computation overhead as shown in Table 5.

Note that the total computation costs for EAP-AKA, EAP-TLS, and EAP-IKEv2 are $2C_{SHA1}+16C_{HM}$, $2C_{CV}+2C_{AS}+1C_{SV}+1C_{DS}+6C_{HM}+4C_{SHA1}$, and $2C_{DH}+2C_{HM}+$

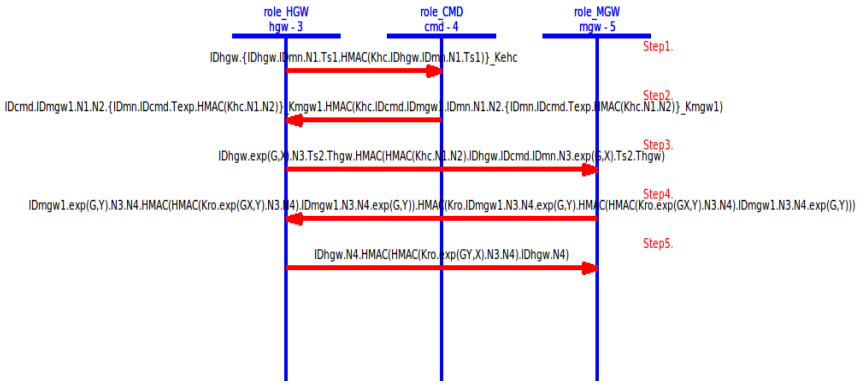


FIGURE 16. The protocol simulation of RO-INIT.

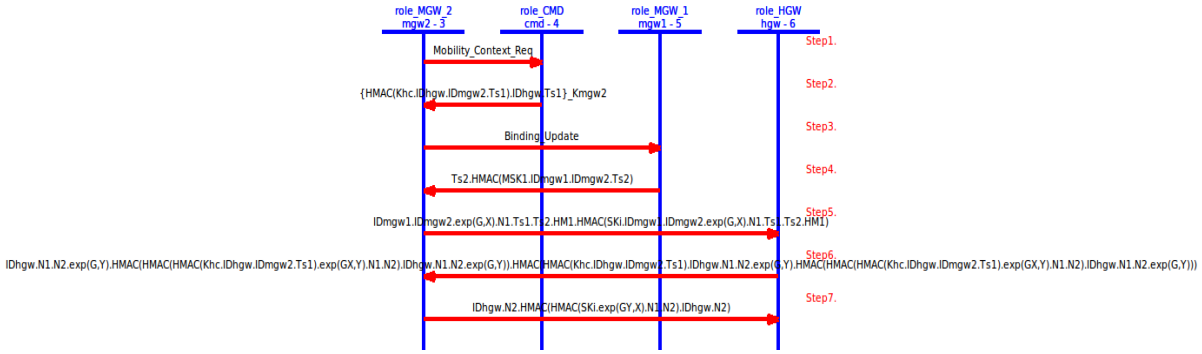


FIGURE 17. The protocol simulation of RO-HO.

TABLE 5. The comparison of the proposed protocol and other standard security protocols in terms of computation overhead.

Scheme	Computation Overhead			
	MGW	CMD	HGW	Total
EAP-AKA	-	$1C_{SHA1} + 8C_{HM}$	$1C_{SHA1} + 8C_{HM}$	$2C_{SHA1} + 16C_{HM}$
EAP-TLS	-	$1C_{CV} + 1C_{AS} + 1C_{SV} + 3C_{HM} + 2C_{SHA1}$	$1C_{CV} + 1C_{AS} + 1C_{DS} + 3C_{HM} + 2C_{SHA1}$	$2C_{CV} + 2C_{AS} + 1C_{SV} + 1C_{DS} + 6C_{HM} + 4C_{SHA1}$
AP-IKEv2	-	$1C_{DH} + 1C_{HM} + 2C_{SYM} + 1C_{DS} + 1C_{SV}$	$1C_{DH} + 1C_{HM} + 2C_{SYM} + 1C_{DS} + 1C_{SV}$	$2C_{DH}+2C_{HM} + 6C_{SYM}+2C_{DS} + 2C_{SV}$
RO_INIT	$5C_{HM} + 1C_{SYM} + 1C_{DH}$	$3C_{HM} + 2C_{SYM}$	$8C_{HM}+1C_{SYM} + 1C_{DH}$	$16C_{HM} + 4C_{SYM} + 2C_{DH}$
RO_HO	$5C_{HM} + 1C_{DH}$	$1C_{HM}$	$7C_{HM} + 1C_{DH}$	$13_{HM} + 2C_{DH}$

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.

$6C_{SYM}+2C_{DS}+ 2C_{SV}$, respectively. Meanwhile, those of the RO-INIT and RO-HO phases are $16C_{HM}+ 4C_{SYM}+ 2C_{DH}$ and $13_{HM}+ 2C_{DH}$, respectively. It is thus observed that the computation cost of the proposed protocol is better than other public key based schemes EAP-TLS and EAL-IKEv2. Even though EAP-AKA has lower computation overhead than others, its security is not enough to support the route in DMM optimization based smart home networks.

Lastly, the communication overhead was also compared among the proposed protocol and other security protocols in terms of roundtrip time. Compared to other protocols, the proposed protocol achieves the best network latency.

VI. CONCLUSION

For 5G emerging smart home networks, it is of paramount importance to provide remote access in a secure and efficient way. Aiming at such remote access, this paper presents a secure route optimization protocol in smart home networks based on DMM that is highly expected to be a major mobility management solution in 5G era. Based on the formal security analysis with BAN-logic and AVISPA, it is proved that the proposed protocol is correct. In addition, the derived 12 lemmas show that it provides mutual authentication, key exchange, perfect forward secrecy, and privacy while defending against the resource exhaustion attack and the attack by malicious MGW. Finally, we can see that the proposed proto-

col in comparative analysis is better than other approaches including EAP-AKA, EAP-TLS, and EAP-IKEv2 given a comprehensive consideration of security properties, computational overhead, and communication overhead. In future, the proposed protocol will be implemented in a real testbed with varying traffic to measure the actual network performance and computation overhead. Moreover, we will extend the proposed protocol to both 5G architectures, Standalone and Non-Standalone.

REFERENCES

[1] J.-H. Lee, J.-M. Bonnin, P. Seite, and C. H. Anthony, "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.

[2] F. Giust, L. Cominardi, and C. J. 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.

[3] C. Perkins, D. Johnson, and J. Arkko, *Mobility Support in IPv6*, document IETF RFC 6275, 2011. [Online]. Available: https://tools.ietf.org/html/rfc6275

[4] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, *Proxy Mobile IPv6*, document IETF RFC 5213, 2008. [Online]. Available: https://tools.ietf.org/html/rfc5213

[5] G. Choudhary, J. Kim, and V. Sharma, "Security of 5G-mobile Backhaul Networks: A survey," *J. Wireless Mobility Netw., Ubiquitous Comput. Dependable Appl.*, vol. 9, no. 4, pp. 41–70, 2018.

[6] M. S. Rahman, A. Basu, T. Nakamura, H. Takasaki, and S. Kiyomoto, "PPM: Privacy policy manager for home energy management system," *J. Wireless Mobility Netw., Ubiquitous Comput. Dependable Appl.*, vol. 9, no. 2, pp. 42–56, 2018.

[7] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You, "Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks," *IEEE Access*, vol. 5, pp. 11100–11117, 2017.

[8] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," *Future Gener. Comput. Syst.*, vol. 86, pp. 740–749, Sep. 2018.

[9] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE Symp. Secur. Privacy*, San Jose, CA, USA, May 2016, pp. 636–654.

[10] A. Brauchli and D. Li, "A solution based analysis of attack vectors on smart home systems," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun.*, Shanghai, China, Aug. 2015, pp. 1–6.

[11] R. J. Robles, T. H. Kim, D. Cook, and S. Das, "A review on security in smart home development," *Int. J. Adv. Sci. Technol.*, vol. 15, pp. 13–22, Feb. 2010.

[12] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Gener. Comput. Syst.*, vol. 56, pp. 719–733, Mar. 2016.

[13] J. Arkko, C. Vogt, and W. Haddad, *Enhanced Route Optimization for Mobile IPv6*, document IETF RFC 4886, 2007. [Online]. Available: https://tools.ietf.org/html/rfc4866

[14] C. E. Perkins, *Securing Mobile IPv6 route optimization using a static shared key*, document IETF RFC 4449, 2006. [Online]. Available: https://tools.ietf.org/html/rfc4449

[15] I. You, "A ticket based binding update authentication method for trusted nodes in mobile IPv6 domain," in *Proc. Int. Conf. Embedded Ubiquitous Comput.* (Lecture Notes in Computer Science), vol. 4809, Taipei, Taiwan, Dec. 2007, pp. 808–819.

[16] I. You, J.-H. Lee, and B. Kim, "caTBUA: Context-aware ticket-based binding update authentication protocol for trust-enabled mobile networks," *Int. J. Commun. Syst.*, vol. 23, no. 11, pp. 1382–1404, Nov. 2010.

[17] S. Krishnan, R. Koodli, P. Loureiro, Q. Wu, and A. Dutta, *Localized Routing for Proxy Mobile IPv6*, document IETF RFC 6705, 2012. [Online]. Available: https://tools.ietf.org/html/rfc6705

[18] K. Xue, L. Li, P. Hong, and P. McCann, *Routing Optimization in DMM*, document, IETF Internet-Draft, 2013. [Online]. Available: https://tools.ietf.org/html/draft-xue-dmm-routing-optimization-02

[19] H. Yang and Y. Kim, *Routing Optimization with SDN*, document, IETF Internet-Draft, 2016. [Online]. Available: https://tools.ietf.org/html/draft-yang-dmm-sdn-dmm-05

[20] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[21] 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. Viganò, and L. Vigneron, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. Int. Conf. Comput. Aided Verification*, (Lecture Notes in Computer Science), vol. 3576, Scotland, U.K., Jul. 2005, pp. 281–285.

[22] V. Sivaraman, H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: Security and privacy implications," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 71–79, Jun. 2018.

[23] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, Jan. 2018.

[24] A. Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," in *Proc. IEEE 2nd World Forum Internet Things*, Milan, Italy, Dec. 2015, pp. 727–732.

[25] J. C. S. Sicato, P. K. Sharma, V. Loia, and J. H. Park, "VPNFilter malware analysis on cyber threat in smart home Network," *Appl. Sci.*, vol. 9, no. 13, p. 2763, 2019.

[26] B. Ali and A. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, 2018.

[27] T. Aura, *Cryptographically Generated Addresses (CGA)*, document IETF RFC 3972, 2005. [Online]. Available: https://tools.ietf.org/html/rfc3972

[28] H. Modares, A. Moravejosharieh, J. Lloret, and R. Bin Salleh, "A survey on proxy mobile IPv6 handover," *IEEE Syst. J.*, vol. 10, no. 1, pp. 208–217, Mar. 2016.

[29] J. Guan, I. You, C. Xu, H. Zhou, and H. Zhang, "Survey on route optimization schemes for proxy mobile IPv6," in *Proc. Sixth Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Palermo, Italy, Jul. 2012, pp. 541–546.

[30] D. Simon, B. Aboba, and R. Hurst, *The EAP-TLS Authentication Protocol*, document IETF RFC 3972, 2008. [Online]. Available: https://tools.ietf.org/html/rfc3972

[31] J. Arkko and H. Haverinen, *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*, document IETF RFC 4187, 2006. [Online]. Available: https://tools.ietf.org/rfc/rfc4187.txt

[32] 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. [Online]. Available: https://tools.ietf.org/rfc/rfc5106.txt

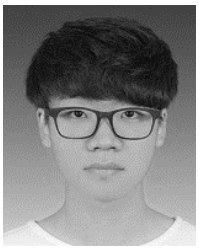
[33] S. Kent, *IP Encapsulating Security Payload (ESP)*, document IETF RFC 4303, 2005. [Online]. Available: https://www.ietf.org/rfc/rfc4303.txt

[34] P. Syverson and I. Cervesato, "The logic of authentication protocols," in *Foundations of Security Analysis and Design* (Lecture Notes in Computer Science), vol. 2171, Bertinoro, Italy, Sep. 2001, pp. 63–137.

[35] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman, "Secure and efficient protocol for fast handover in 5G mobile Xhaul networks," *J. Netw. Comput. Appl.*, vol. 102, pp. 38–57, Jan. 2018.

[36] I. You, Y. Hori, and K. Sakurai, "Enhancing SVO logic for mobile IPv6 security protocols," *J. Wireless Mobility Netw., Ubiquitous Comput. Dependable Appl.*, vol. 2, no. 3, pp. 26–52, 2011.

DAEMIN SHIN received the M.S. degree from Korea University, South Korea, in 2009. He is currently pursuing the Ph.D. degree with the Department of Information Security Engineering, Soonchunhyang University, South Korea. He is also with the Financial Security Institute, as the Manager. His current research interests include the mobile Internet security, the IoT security, and financial security.



KEON YUN received the B.S. degree in information security engineering from Soonchunhyang University, South Korea, where he is currently pursuing the master's degree with the Department of Information Security Engineering. His current research interests include the mobile Internet security, 5G, formal security analysis, and the IoT security.

JIYOON KIM received the M.S. degree in information security engineering from Soonchunhyang University, South Korea, where he is currently pursuing the Ph.D. degree with the Department of Information Security Engineering. His current research interests include the 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 Soochunhyang University, South Korea.

From 2009 to 2015, he worked as a Lecturer with the University of San Carlos. From 2014 to 2015, he was a Research Assistant with the Phil-LiDAR Program. From 2015 to 2016, he was a Research Assistant with the Sensor Laboratory, Clemson University, Clemson, SC, USA. His research interests include sensor development, embedded system design and development, the mobile Internet security, and the IoT security.

JEONG-NYEO KIM received the M.S. and Ph.D. degrees in computer engineering from Chungnam National University, South Korea, in 2000 and 2004, respectively. She studied computer science from the University of California, Irvine, CA, USA, in 2005. Since 1988, she has been a Principal Member of Engineering Staff with the Electronics and Telecommunications Research Institute (ETRI).

ILSUN YOU (M'12–SM'13) 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 the Internet security, authentication, access control, and formal security analysis. He is a Fellow of the IET. He is the EiC of the *Journal of Wireless Mobile Networks*, *Ubiquitous Computing*, and the *Dependable Applications* (JoWUA), and the *Journal of Internet Services and Information Security* (JISIS). He is on the Editorial Board of the *Information Sciences*, the *Journal of Network and Computer Applications*, the *International Journal of Ad Hoc and Ubiquitous Computing, Computing and Informatics*, the *Intelligent Automation and Soft Computing*, and so on.