IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

SPECIAL SECTION ON SECURITY AND PRIVACY IN APPLICATIONS AND SERVICES FOR FUTURE INTERNET OF THINGS

Received April 1, 2017, accepted April 18, 2017, date of publication June 1, 2017, date of current version July 3, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2710379

Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks

DAEMIN SHIN[1,2], VISHAL SHARMA[1], JIYOON KIM[1], SOONHYUN KWON[1], 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

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

This work was supported in part by the National Research Foundation of Korea, Ministry of Education, through the Basic Science Research Program, under Grant 2016R1D1A1B03935619, and in part by the Soonchunhyang University Research Fund.

ABSTRACT The communication in the Smart Home Internet of Things (SH-IoT) comprising various electronic devices and sensors is very sensitive and crucial. In addition, the key requirements of the SH-IoT include channel security, handover support, mobility management, and consistent data rates. Proxy mobile IPv6 (PMIPv6) is considered as one of the core solutions to handle extreme mobility; however, the default PMIPv6 cannot ensure performance enhancement in SH-IoT scenarios, i.e., Route Optimization (RO). The existing security protocols for PMIPv6 cannot support secure RO for smart home IoT services, where mobile nodes (MNs) communicate with home IoT devices not belonging to their domain. Motivated by this, a secure protocol is proposed, which uses trust between PMIPv6 domain and smart home to ensure security as well as performance over the path between MNs and home IoT devices. The proposed protocol includes steps for secure RO and handover management, where mutual authentication, key exchange, perfect forward secrecy, and privacy are supported. The correctness of the proposed protocol is formally analyzed using BAN-logic and Automated Validation of Internet Security Protocols and Applications (AVISPA). Furthermore, network simulations are conducted to evaluate the performance efficiency of the proposed protocol. The results show that the proposed approach is capable of providing secure transmission by resolving the RO problem in PMIPv6 along with the reduction in handover latency, end to end delay and packet loss, and enhancement in throughput and transmission rate even during the handover phase.

INDEX TERMS Route optimization (RO), handovers, security, smart home, IoT.

I. INTRODUCTION

The evolution of new communication technologies in the electric and electronic industry gives a broader vision to control and operate various types of equipment in a home. The involvement of enhanced electronic gadgets, which can be operated by understanding the signals, allows the formation of a smart home. A smart home consists of various electronic devices which can relay information to a smart home application interface by using a communication channel as shown in Fig. 1.

Further, the evolution of Internet of Things (IoT) has enhanced the actual implementation of networked smart homes. With easy to operate smart home expansion systems by using IoT devices, life has become convenient, comfortable, and secure. Also, the major role has been the flexibility in management, cost-saving, and reduced energy consumption. Some of the applications of Smart Home-IoT (SH-IoT) network implementation include surveillance using cameras, leak detections, air concentration check, and temperature control, etc.

The smart home aims at forming an energy optimized environment, which can efficiently regulate the use of various IoT devices. A smart home reduces the burden of excess operations as well as saves per device energy consumption in a home, which lays a ground for greener communication. Currently, the large network operators have standardized the workflow for managing the operations of various SH-IoT devices. Using different communication standards and dedicated smart home apps, the IoT devices can be easily controlled and monitored.

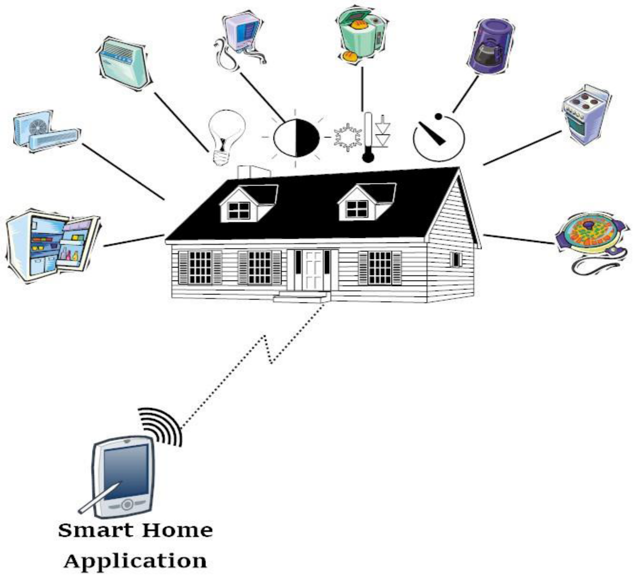


FIGURE 1. An illustration of a smart home equipped with various IoT devices.

Despite the advantages of SH-IoT networks in providing automation facilities, there are certain limitations and challenges associated with their efficient deployment. The data between the IoT devices and the controller, which is a remote node operating as an application interface on the users' device, moves through a series of anchors and gateways. This flow of data needs an optimal path without any excessive transmission overheads to instantly control the devices. Thus, Route Optimization (RO) is one of the major challenges for the SH-IoT networks. The traffic over SH-IoT networks is very sensitive for timeliness, security, and privacy. This is because such traffic is expected to be generated by advanced multimedia applications such as augmented reality as well as the personal smart home applications including health care and home surveillance, etc. There are many approaches which provide security in terms of privacy and authentication, but these also add up to the excessive delay in transmission. Thus, tradeoff between security and time of operation must be efficiently handled in the network aiming at RO.

Device fingerprinting can be one of the solutions, as suggested by Jose *et al.* [1], for providing home automation security. Such solutions can be used to detect the devices which request or make a connection with the home automation setup, however, timeliness and authentication delay are still a concern in this approach. Focus on the state and context of operation can provide sufficient support for enhancing the security of home automation systems [2]. However, selection of a route using an intermediate anchor can still cause much delay in authentication. Context-aware privacy can eliminate the risk of attacks over the SH-IoT devices. This can be easily attained by using more powerful and cheap sensor devices, which can provide context-based situational awareness allowing the network to automatically select the security feature for improving the transmission without compromising its services. However, the addition of extra sensors for context awareness may further elongate the transmission path, which may lead to various performance overheads [3].

Use of light weight and secure session key approach can also provide security in smart homes [4]. Multilevel authentication can be a strong solution to security and privacy issues in smart home automation systems [5]. Distributed security solutions can also enhance the channel security of smart homes operating with a large number of IoT devices [6]. However, despite the level of security provided by the existing approaches, performance of the network suffers a lot due to the involvement of multiple and periodic updates among the network entities. Further, the existing solutions leverage excessive burden on the network during handovers, as these do not consider any optimization strategy to counterfeit the excessive overheads of handovers. Thus, an efficient approach is required, which not only enhances the security and privacy of the network allowing secure transmission between the SH-IoT devices and the smartphone application, but also provides better performance in terms of handover latency, delivery ratio, and end to end delays.

A. BACKGROUND AND PROBLEM STATEMENT

As shown in Fig. 2, the default Proxy Mobile IPv6 (PMIPv6) based SH-IoT networks allow a Mobile Node (MN) to communicate with Corresponding Nodes (CNs), which are SH-IoT devices in its home, regardless of its location and movement via two intermediate entities, namely, Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA) [61]. In PMIPv6 based SH-IoT networks, a smart home is composed of a Home Gateway (HGW) and SH-IoT devices, and each device relies on the HGW to communicate with external entities including MNs. From Fig. 2, it can be noticed that every message, which is to be transferred to/from the CN, follows a non-optimal path among the MAG, the LMA, and the HGW leading to excessive performance overheads. In addition, whenever a handover decision is made, repetition of the entire procedure through the path MAG-LMA-HGW increases the handover latency, which affects the performance of the entire network. The above mentioned problems raise the requirement of the RO. Here, it is worth to note that the RO, if not secured adequately, is vulnerable to various security threats [30]. Considering security aspects, there are three possible trusts established in the default PMIPv6 based SH-IoT networks: trust between MN and MAG, trust between MAG and LMA, and trust between HGW and CN. Unfortunately, these trusts are not enough to achieve secure RO because they cannot allow a MAG and a HGW to authenticate each other and negotiate a session key. In other words, it is impossible to provide secure RO based on the current possible trusts. Thus, elimination of the excessive dependency over the LMA (triangular routing) for every transmission, even after the authentication, is the problem statement as well as motivation behind the requirement of a new solution for secure RO in smart home applications.

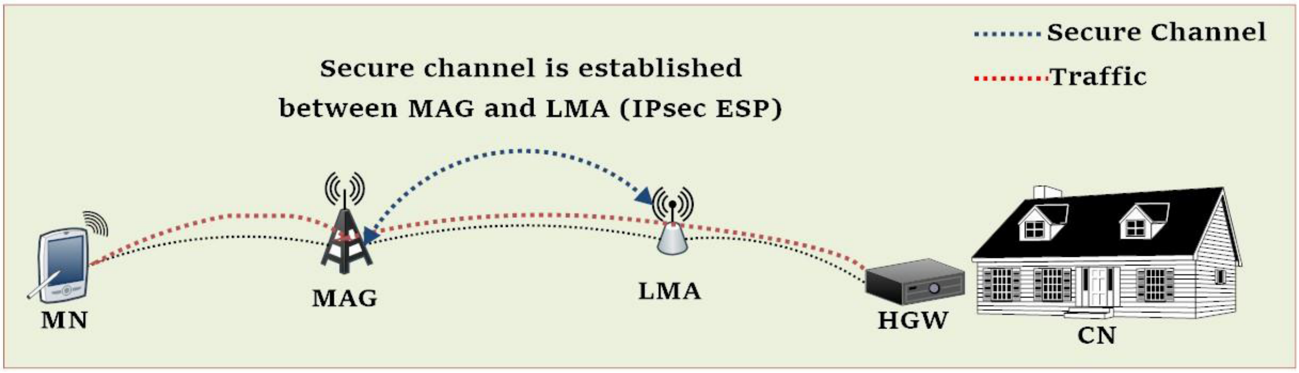

Secure Channel
Traffic
Secure channel is established
between MAG and LMA (IPsec ESP)
MN
MAG
LMA
HGW
CN

FIGURE 2. The default PMIPv6 based SH-IoT networks.

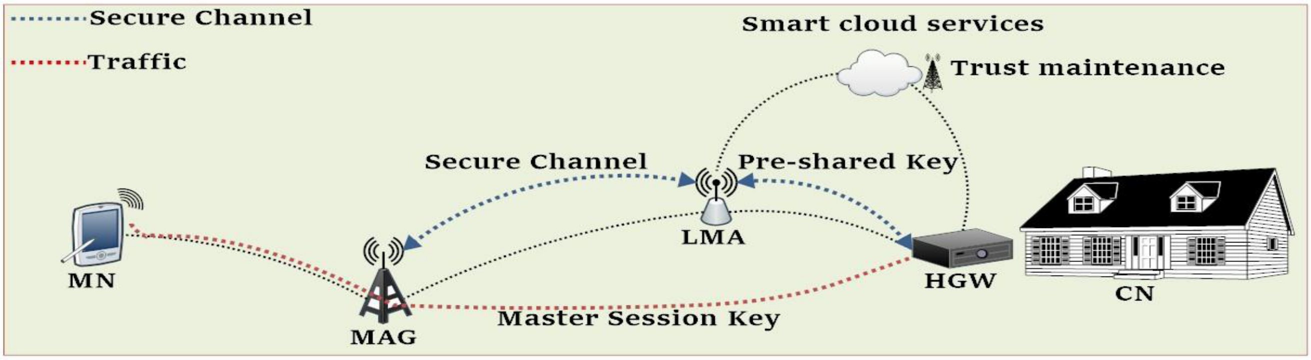


FIGURE 3. The proposed PMIPv6 based SH-IoT networks. The trust between LMA and HGW is maintained by using the smart cloud services from the network providers. Note that the 4 session keys are established between MAG and HGW • SK_i (or SK_i): This key is derived from $K_{LMA-HGW}$ by HGW, and forwarded to MAG through RO-INIT or PBA. Its main purpose is to protect EBU and EBA (Diffie-Hellman Key exchange) • *MSK*: this is a master session key, which is exchanged based on Diffie-Hellman, and thus provides PFS. It is also used to derive AK and EK. • *AK*, *EK*: these keys are used to protect the data's authenticity and confidentiality.

B. OUR CONTRIBUTION AND HIGHLIGHTS

In this paper, the problem of secure RO is considered for a SH-IoT. The task of eliminating the excessive dependency over the LMA is handled on the basis of the pre-established trust between the HGW and the LMA, which can be achieved by the smart home users with the help of smart home cloud services. That is, the proposed approach counts on the pre-shared key between the LMA and the HGW to provide mutual authentication and secure session key exchanges, as shown in Fig. 3. Among the established session keys, the first key, derived from the pre-shared key, is used to protect the Diffie-Hellman Key exchange for the second one, which is the master session key. Note that the master session key is established in a way for supporting Perfect Forward Secrecy (PFS) [68] as well as is used to derive the last two session keys, which protect the confidentiality, authenticity, and privacy of the exchanged data between the MN and the CN. The key highlights of the proposed solution are:

1. Secure transmission between the MN and the CN along with route optimization.

2. Lower handover latency and high delivery ratio along with a high probability of handovers.

3. Formal security analysis on the proposed security protocol.

II. RELATED WORK

Security in smart home has always been a concern for most of the applications. Over the last decade many researchers have evaluated various aspects of security in smart home automation as well as routing. Smart homes operate on critical sensors, which are to be secured for timely connections with the controlling nodes using security and privacy approaches [7], [8]. On the other hand, there have been considerable studies for RO in MIPv6 and its extensions including PMIPv6 [61]. In this paper, the literature is presented by dividing the available solutions into three major parts, namely, standalone security approaches for smart home security, RO solutions following MIPv6, and RO with PMIPv6.

A. SMART HOME SECURITY

Smart home security deals with the protection of communication between the smart home sensors and apps running on a mobile device. The security ranges from data security to channel security. Cloud computing can provide a varied platform for securing transmission between the users and the smart home sensors.

Wang *et al.* [9] designed a security system for smart homes using cloud computing environment. The authors emphasized on the use of intermediate hops as a platform to secure the transmission between the nodes. However, using excess hops causes many overheads despite the level of security. Madakam *et al.* [10] discussed the security approaches for connectivity between the smart devices in IoT environment. The authors emphasized on both physical as well as logical remedies for security enhancement. Security over IoT devices is discussed at large by the authors. Brauchli *et al.* [11] conducted analyses of attack vectors in smart home systems. The authors ranked the attack vectors in smart homes and evaluated the usability impact of different attacks.

Jacobsson *et al.* [12], [13] conducted risk analyses of smart home automation systems and identified 32 different risks in these systems. The authors evaluated human interaction behavior as the key component for the majority of risks in smart home systems. However, the authors did not discuss much on the security solutions of the identified risks. Ge *et al.* [14] developed a framework for the security evaluation of IoT devices. The authors designed a five-phase model which is evaluated using three different scenarios. The authors evaluated the attacker paths and mitigated the impact of attacks. However, features related to performance evaluations and communication overheads are not considered while developing the framework.

Mehdi *et al.* [15] used OpenFlow to define security framework for smart home IoT networks. The authors used software-defined solutions to provide a modular and flexible solution for building smart intrusion detection system focusing on smart homes. Fernandes *et al.* [16] detected privacy sensitive situations of smart homes primarily focusing on social robots. The authors' work revolves around the user movement where smart robot detects a possible state of intrusion. Low scope, non-evaluation of communication channel, and inefficient passage of data between mobile nodes and sensors make this solution applicable to limited scenarios.

B. ROUTE OPTIMIZATION WITH MIPv6

MIPv6 provides support for bidirectional tunneling and RO in the mobile networks. For the protection of binding updates, IETF focuses on the use of Return Routability (RR) approach [17]. This method aims at coordinating the RO between the CN and MN. Apart from this, considering the environments where MNs can establish trust with CNs, static shared key (SSK) protocol is used as specified by the IETF [18]. RO with MIPv6 involves heavy dependency on the binding update before the initiation of handovers [19]. Several approaches are proposed by different authors over the years to resolve issues concerning RO in MIPv6.

Ren *et al.* [20] discussed the security for RO in MIPv6. The authors proposed a lightweight binding update protocol to enhance the security during routing. The approach developed by the authors uses public key certificate-based strong authentication. Kavitha *et al.* [21] also evaluated the security of the binding update based protocols for RO in MIPv6. The authors categorized their analyses in two parts, one for the RR protocols and other for the Certificate based Binding Update (CBU) protocols. Different attack environments are considered by the authors for evaluating these protocols. Song et al. [22] developed a secure and lightweight application for RO. The authors focused on preventing session hijacking attack by mode of authenticating a suspicious message. Their approach provides less computational overheads for detecting session hijacking attacks.

Hawi *et al.* [23] developed an identity-based solution for RR procedures to eliminate the drawbacks of triangular routing. Mehdizadeh *et al.* [24], [25] gave secure RO solution while emphasizing on the data integrity of the network. The proposed work by the authors uses strong and light data encryption. Their approach is capable of providing safe and secure data communication between the CNs and MNs. Rossi *et al.* [26] developed a secure RO solution which uses enhanced cryptographically generated address (ECGA) based on a backward key chain, which links multiple CGAs together. Diana *et al.* [27] developed a new discovery mechanism to eliminate the latency in home registration procedures in MIPv6 networks. The authors improved the discovery procedure for Home Agents (HA) in comparison with the default MIPv6. However, excessive iteration during authentication and packet delay may easily be induced in their work because of distance manipulation by an intruder. Taha *et al.* [28] developed an anonymous and location preserving scheme for MIPv6 in heterogeneous networks. Their approach provides low communication overheads and low packet delays. However, their approach suffers from pairing authentication delays which can affect the performance of a network.

Further, You [29] developed a ticket based binding update authentication (TBUA) procedure which improves the SSK protocol by using an HA as a ticket server. The working procedure of this protocol is divided into three phases, namely, ticket binding phase, early binding phase, and complete binding phase. This approach is capable of reducing the cost involved in pre-configuring and maintenance of key materials. The TBUA protocol suffers from a major issue of security and efficiency in managing MNs' Care of Address (CoA). This issue is eliminated in the updated version of TBUA, which is given as caTBUA again by You *et al.* [30]. The authors introduced the features of context awareness to the TBUA in order to secure the CoA during the second phase of authentication. caTBUA provides better performance in terms of authentication cost and message transmission latency.

C. ROUTE OPTIMIZATION WITH PMIPv6

PMIPv6 provides mobility support to MNs without depending on MNs for signaling [31], [32]. The use of LMA and MAG is fully considered in the PMIPv6. Similar to MIPv6, RO is a major concern in PMIPv6, which has seen a lot of researches over the past few years. Most of the existing solutions have focused on new ideology for optimizing the route and lowering the handover latency by using PMIPv6 in different network scenarios.

Raza *et al.* [33] provided software-defined RO for PMIPv6. The authors focused on optimizing the transmission path by reducing the handover and transmission delays. Kim *et al.* [34] developed a proactive correspondent registration approach for PMIPv6 RO. Their approach is capable of reducing registration latency by performing attachment procedures before the actual handovers. Leu *et al.* [35] proposed an intra-LMA model for mobility management in PMIPv6 networks. The authors utilized stream control transmission protects mechanism along with RO to reduce the end to end delay and lower the packet loss rate. Han *et al.* [36] performed RO by using routing table of MAG. The authors also used the security database of MAG to enhance the performance of a PMIPV6 network. Chiba *et al.* [37] worked on the IP multimedia networks and considered RO over these networks. The authors emphasized on reducing the data path between the communicating nodes in order to optimize the traffic flow. Choi *et al.* [38] used correspondent information for RO. The authors used corresponding binding updates which provide bi-path communication between the MAG and LMA. Kang *et al.* [39] emphasized on a reliable packet transmission to optimize the route. The authors compared their work with the default PMIPv6 and out-of-sequence time period scheme. Their approach is capable of providing reliable communication by overcoming the issue of out-of-sequence. However, despite the advantages of these approaches for RO in PMIPv6, most of the existing solutions do not consider the security aspect, which makes the network vulnerable to many attacks allowing intruders to further impact the performance of the network.

Another aspect of RO in PMIPv6 is the handover management and localization [40]–[43]. Many approaches have been developed over the years which dedicatedly focused on handover issues along with RO in PMIPv6 networks. Raseem *et al.* [44], [45] provided efficient handover mechanism along with localized routing. The authors provided a solution for optimized localization, which provides lower handover delays and allows high network utilization. Cho *et al.* [46] conducted performance analyses of inter-domain handovers over virtual layers in PMIPv6 based IoT. The approach provided by the authors reduces the signaling traffic during location updates which result in lower handoff latency and better binding update rate. Efficient handover management and locality in PMIPv6 can readily resolve the issues of tunneling as well as RO [47]–[51]. However, these solutions need to incorporate security measures to perform an actual evaluation of handover metrics for fully sustainable, efficient, and secure transmission in PMIPv6 networks.

Securing communication and RO are two of the key challenges in PMIPv6 networks [52]. Most of the existing approaches consider a single parametric improvement and provides a solution over a limited set of parameters, thus, opening a wide scope for further enhancements. Magagula and Chan [53] provided early discovery mechanisms and pre-authentication in order to reduce the handover delays in PMIPv6 networks. The authors emphasized on using 802.21 to overcome the handover latency in proxy networks. Tripathi *et al.* [54] provided secure authentication to reduce the packet loss. The authors compared their work with the default MIPv6 and PMIPv6. Gao *et al.* [55] developed a scheme on the basis of identity-based signature to provide low communication overheads during mutual access authentication. You *et al.* [56] developed an adaptive authentication scheme for mobile devices operating with PMIPv6. The authors primarily considered MN's context information for taking a decision on the authentication strength. The developed context-aware solution is capable of providing security and efficiency simultaneously. Although, the level of support provided by this protocol in comparison with the existing binding update solutions is efficient, yet not sufficient enough to support the performance level as demanded in the smart home security. A detailed comparison between various RO approaches is provided in Table 1.

III. PROPOSED PROTOCOL: SECURE AND EFFICIENT ROUTE OPTIMIZATION

The proposed protocol consists of two steps: the Route Optimization Initialization (RO_INIT) and Handover Management (RO_HO_MAN) steps. In the former, the route optimization is initialized. The latter manages a route optimization mode in the handover process. The symbols used to describe the proposed protocol are shown in Fig. 4.

The assumptions considered in the development of the proposed protocol are as follows:

- It is assumed that there is a smart home cloud service associated with the PMIPv6 domain of the MN. The MN user subscribes to the smart home cloud service and establishes a trust relationship between the PMIPv6 domain and the HGW by registering its HGW with the service provider. As a result of this trust relationship, the secret key $K_{LMA-HGW}$ is shared between the PMIPv6 domain and the HGW and stored in the policy store of the PMIPv6 domain and the HGW.
- It is assumed that the communication between the MAG and the LMA is protected on the basis of IPsec Encapsulating Security Payload (ESP) [IETF RFC 4303 [60]] in a way that it maintains the integrity and confidentiality of the communication. This corresponds to the security considerations defined in the PMIPv6 standard document. [RFC5213 [61]]
- It is assumed that the secure channel between the previous and new MAGs is pre-established based on IPsec ESP. Therefore, the handover and RO context of the MN can be securely transmitted from the previous MAG to the next one.

The security characteristics targeted by the proposed protocol are as follows.

- Mutual authentication: Mutual authentication between the HGW and the MAG (or nMAG) must be supported to provide RO.
- Key exchange: The session key between the HGW and the MAG must be exchanged to protect the path optimization process and subsequent data transmission.
- Perfect Forward Secrecy (PFS): Since the security of the data exchanged between the MN and the CN is very

TABLE 1. Comparison of various RO approaches for MIPv6 and PMIPv6. (*discussed but not provided explicitly).

Approach	Ideology	Author	Version	Handover Support	Triggering Entity	Security	Back Compatibility
IETF RFC 4449	Secure route optimization	Perkins [17]	MIPv6	-	-	Yes	-
RO in MIPV6	Light weight BU protocol	Ren et al. [20]	MIPv6	Yes	MN	Yes	-
Secure RO	Mitigating session Hijacking	Song et al. [22]	MIPv6	Yes	MN	Yes	-
Secure framework for RO	Return routability procedure	Al Hawi et al. [23]	MIPv6	Yes	MN	Yes	-
Data Integrity in RO	Light data encryption	Mehdizadeh et al. [24]	MIPv6	-	-	Yes	-
Secure RO	Enhanced CGA and DNSSEC	Rossi et al. [26]	MIPv6	Yes	MN	Yes	-
Adaptive authentication	Context based adaptive authentication scheme	You et al. [56]	PMIPv6	Yes	MAG	Yes	Yes
Hierarchical IBS for proxy mobile IPV6	Access authentication scheme	Gao et al. [55]	PMIPv6	Yes	MAG	Yes	Yes
Localized routing problem	Tunnel maintenance	Liebsch and Jeong [57]	PMIPv6	Yes	LMA	Yes	Yes
Localized routing	IPv4 Support for PMIPv6	We et al. [58]	PMIPv6	Yes	MAG/LMA	Yes*	Yes
Localized routing	Localized forwarding and direct tunneling	Krishnan et al. [59]	PMIPv6	Yes	MAG/LMA	Yes*	Yes

important, the session key for protecting the data transmission during the key exchange must be supported with PFS, i.e., even if the long term key, $K_{LMA-HGW}$, or the current or successive session key is leaked out, the past session key for data protection should not be restored.

- Privacy: The MN's identity should not be revealed in the message for RO between the MAG and the HGW.
- Defense against resource exhaustion attacks: The resource exhaustion attack is a kind of Denial of Service (DoS) attack attempting to cause victims' resources to be occupied in vain. The proposed approach should not be vulnerable to these DoS attacks that cause the involved entities to suffer from excessive public key operations [62].
- Defense against attacks by malicious MAGs: The proposed solution should not be vulnerable to a redirection attack by a malicious MAG.

In order to provide the above security properties, the proposed protocol protects the RO on the basis of a trust relationship between the MN's HGW and PMIPv6 domains where the session key exchange is performed using Diffie-Hellman. To this end, it supports the mutual authentication between the MAG and the HGW as well as the exchange of the session key with PFS.

A. ROUTE OPTIMIZATION INITIALIZATION STEP (RO_INIT)

The RO_INIT process determines if the route is optimized after initiation of the PMIPv6 Binding Update process, as shown in the Fig. 5. It is activated if the MN has the right to perform such a routing (selection of next hop).

In this process, the PMIPv6 entities, MN, MAG and LMA, perform authentication and binding update like the existing PMIPv6 before RO decision. When the binding update is successfully completed, the LMA accesses the Policy Store of the PMIPv6 domain to obtain the HGW information (HGW address, secret key $K_{LMA-HGW}$, route optimization policy, etc.) that is related to the MN. The details of the procedures shown in Fig. 5 are explained below:

(1) It is assumed that the LMA has the pre-established trust with the smart home served by an HGW where the CN makes a connection with the MN. If the MN has the appropriate

MN, MAG, LMA, HGW, CN	mobile node, mobile access gateway, local mobility anchor, home gateway, and corresponding node
$pMAG$ and $nMAG$	current and next MAGs
RA	Route Advertisement messages
HO_CTX	Handover Context Message
HI and $HAck$	Handover Initiate and Handover Acknowledgement messages
PBU and PBA	Proxy Binding Update and Acknowledgement messages
RO-$INIT$ and RO-ACK	Route Optimization Initialization and Acknowledgement messages
EBU and EBA	Early Binding Update and Acknowledgement messages
CBU	Complete Binding Update message
ID_X, AD_X, HNP_X	public identifier, IPv6 address, and home network prefix of X
n_1 and n_2	randomly generated nonces
ts	timestamp
$K_{LMA\text{-}HGW}$	a pre-shared key between LMA and HGW
$h(m)$	one way hash value on the message m
$HMAC(k, m)$	a hash-based message authentication function where m is an input message and k is a secret key
$E(k, m)$	the message m is encrypted under the key k
Seq	the sequence number
SK_i	the ith session key between HGW and the ith MAG
$\|\|$	concatenation operation

FIGURE 4. Notations and symbols for the proposed approach.

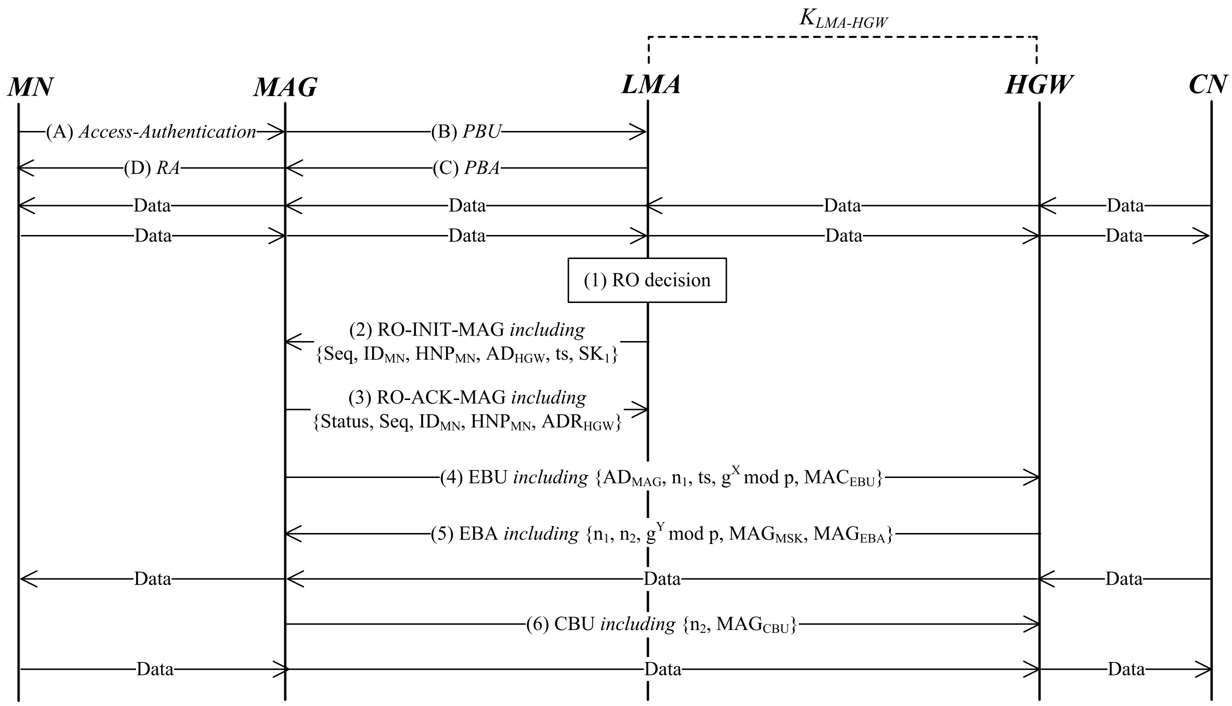
rights to perform RO, then the traffic is observed to determine whether RO between the two is necessary or not.[1]

(2)-(3) At first, the LMA exchanges the RO-INIT and RO-ACK messages with the MAG to initialize the RO process and give the session key, SK_1. Then, the MAG generates a random number n_1 and its own Diffie-Hellman private key X, obtains a public key by $g^X mod\, p$ corresponding to X (where p is prime, and g is a primitive root modulo p), and transmits a created Early Binding Update (EBU) message to the HGW for early binding. Here, the EBU message is protected by the MAG_{EBU}, which is generated from $HMAC(SK_1, ID_{MN} \| HNP_{MN} \| EBU)$. Upon the receipt of EBU message, the HGW first verifies whether the timestamp ts contained in the message is within a valid range around the current time or not. When the verification is completed, the HGW obtains SK_1 by alternately substituting the MN's ID and HNP, which is registered in the HGW, and finds the corresponding MN by verification, since the EBU message does not include the information for identifying the MN (i.e., the privacy of the MN is maintained). This process is an additional overhead for protecting the privacy of the MN. In general, assuming that one HGW is installed in one smart home, the number of registered MNs is very small, and hence, the cost can be ignored. If the verification of MAG_{EBU} is successful, the HGW identifies the MN and trusts for the MAG. Then, it generates its own Diffie-Hellman private key Y and public key by $g^Y mod\, p$ on the basis of the trust. Here, if the HGW does not authenticate the MAG_{EBU}, the HGW can respond to a resource exhaustion attack because the protocol does not allow forwarding of the process. In a valid case, the HGW computes $g^{XY} mod\, p$ using the public key $g^X mod\, p$ of the MAG and its own private key, and generates $MSK = h\left(g^{XY} modp \|n_1\| n_2\right)$ through the resultant value, the random number n_1 received from the MAG, and the random number n_2 generated by the MAG. Also, in order to protect the traffic between the MN and CN, an encryption session key EK and an authentication key AK are generated on the basis of MSK. Here, the Diffie-Hellman public key pair of the MAG and the HGW, which is used to generate the session keys MSK, EK and AK, can be completely discarded after using them only once in a session; this provides PFS.

(4) The HGW sends its correspondent MAG an EBA message that consists of two MAC values, MAG_{MSK} and MAG_{EBA}, along with n_1, n_2, and $g^Y mod\, p$.

In order for the MAG to verify the $MAG_{MSK} = HMAC(AK, ID_{MN} \|HNP_{MN}\| n_1 \|n2\| h(SK_1))$, an AK related public key operation is required. Therefore, the $MAG_{EBA} = HMAC(SK_1, ID_{MN} \|HNP_{MN}\| EBA)$ is used to cope up with the resource exhaustion attack, i.e., when the MAG receives the EBA message, it verifies whether the n_1 included in the message matches with the value held by it (*i.e,* it checks the freshness of the message), and then it attempts to verify the MAG_{EBA} using SK_1. If the validation is successful, the MAG obtains the session keys MSK, AK, and EK through its own private key X and the public key $g^Y mod\, p$

[1] Details on how to decide whether it is necessary to perform the route optimization are beyond the scope of this paper and are not mentioned here.



$K_{LMA\text{-}HGW}$
MN
MAG
LMA
HGW
CN
(A) Access-Authentication
(B) PBU
(D) RA
(C) PBA
Data
(1) RO decision
(2) RO-INIT-MAG including {Seq, ID_{MN}, HNP_{MN}, AD_{HGW}, ts, SK_1}
(3) RO-ACK-MAG including {Status, Seq, ID_{MN}, HNP_{MN}, ADR_{HGW}}
(4) EBU including {AD_{MAG}, n_1, ts, g^X mod p, MAC_{EBU}}
(5) EBA including {n_1, n_2, g^Y mod p, MAG_{MSK}, MAG_{EBA}}
(6) CBU including {n_2, MAG_{CBU}}

* $SK_1 = h(K_{LMA\text{-}HGW}||ts||ID_{MN}||HNP_{MN}||AD_{MAG}||AD_{HGW}||\text{"Session Key"})$
$MAG_{EBU} = HMAC(SK_1, ID_{MN}||HNP_{MN}||EBU)$
X and Y : the Diffie-Hellman private keys of MAG and HGW
$MSK = h(g^{XY} \bmod p||n_1||n_2)$
$EK = h(MSK||n_1||n_2||\text{"Encryption Key"})$
$AK = h(MSK||n_1||n_2||\text{"Authentication Key"})$
$MAG_{MSK} = HMAC(AK, ID_{MN}||HNP_{MN}||n_1||n_2||h(SK_1))$
$MAG_{EBA} = HMAC(SK_1, ID_{MN}||HNP_{MN}||EBA)$
$MAG_{CBU} = HMAC(AK, CBU)$

FIGURE 5. First phase of the proposed approach for RO (RO Initialization Step (RO_INIT Step)).

of the HGW, and verifies whether the MAG_{MSK} is valid based on the AK. If MAG_{MSK} is valid, the MAG trusts the HGW, and at the same time, it confirms that the three keys are securely shared with the HGW.

(5) The MAG completes the RO initialization phase by sending the CBU message containing n_2 and MAG_{CBU} to the HGW. When the HGW receives the CBU message, it verifies the freshness of the message by checking that n_2 included in the message matches the value held by the HGW, and verifies the $MAG_{CBU} = HMAC(AK, CBU)$ value through AK. If the validation is positive, the HGW can confirm that the session keys MSK, AK, and EK are securely shared with the MAG.

B. HANDOVER MANAGEMENT STEP (RO_HO_MAN STEP)

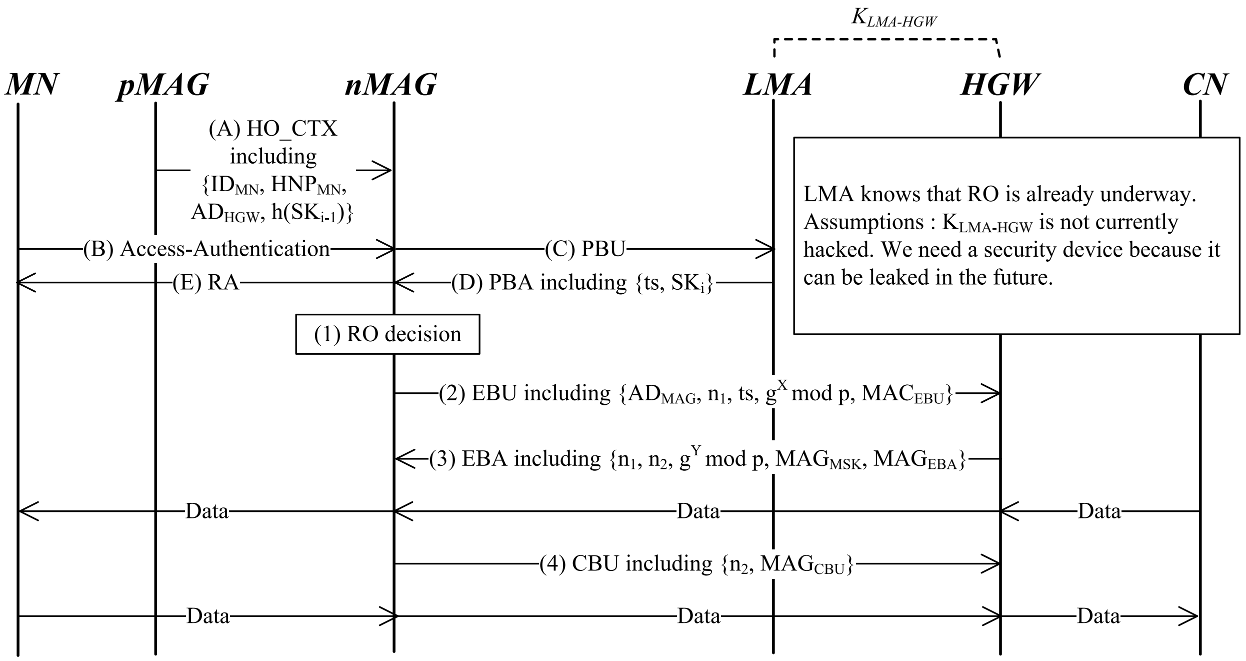
This step supports the RO state of the MN for continuity and safety when the MN performs a handover to another network. The RO_HO_MAN procedures as show in Fig. 6 are explained below:

(1) Before handover from the pMAG to the nMAG by the MN, the pMAG transmits an HO_CTX message including ID_{MN}, HNP_{MN}, AD_{HGW}, and the hash value of the previous session key SK_{i-1} to the nMAG.

(2) - (5) processes show that the MN's authentication process and the standard binding update procedure are performed among the MN, nMAG, and LMA. However, it is different from the standard PMIPv6 operation as the LMA includes the ts and the current session key SK_i in the PBA message sent to the nMAG, thereby allowing SK_i to be shared between the nMAG and the HGW. As the steps (1) - (3) are substantially similar to the steps (3) - (5) of the RO_INIT step, the detailed description is omitted.

IV. SECURITY ANALYSIS

This section presents the formal analyses of the proposed protocol. For this goal, the correctness is verified through BAN-logic [63], which is one of the most popular security analysis tools [64]–[66]. Then, Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [69], a state-of-the-art push-button tool for the automated security validation, is used to check whether the proposed protocol is vulnerable to any attack or not. The synergy


$K_{LMA-HGW}$
MN
pMAG
nMAG
LMA
HGW
CN
(A) HO_CTX including {ID_{MN}, HNP_{MN}, AD_{HGW}, $h(SK_{i-1})$}
(B) Access-Authentication
(C) PBU
(E) RA
(D) PBA including {ts, SK_i}
(1) RO decision
(2) EBU including {AD_{MAG}, n_1, ts, g^X mod p, MAC_{EBU}}
(3) EBA including {n_1, n_2, g^Y mod p, MAG_{MSK}, MAG_{EBA}}
Data
Data
Data
(4) CBU including {n_2, MAG_{CBU}}
Data
Data
Data

LMA knows that RO is already underway. Assumptions : $K_{LMA-HGW}$ is not currently hacked. We need a security device because it can be leaked in the future.

* $SK_i = h(K_{LMA-HGW}||ts||ID_{MN}||HNP_{MN}||AD_{nMAG}||AD_{HGW}||\text{"Session Key"})$
$MAG_{EBU} = HMAC(SK_i, ID_{MN}||HNP_{MN}||h(SK_{i-1})||EBU)$
X and Y : the Diffie-Hellman private keys of MAG and HGW
$MSK = h(g^{XY} \bmod p||n_1||n_2)$
$EK = h(MSK||n_1||n_2||\text{"Encryption Key"})$
$AK = h(MSK||n_1||n_2||\text{"Authentication Key"})$
$MAG_{MAG} = HMAC(AK, ID_{MN}||HNP_{MN}||n_1||n_2||h(SK_{i-1}))$
$MAG_{EBA} = HMAC(SK_i, ID_{MN}||HNP_{MN}||EBA)$
$MAG_{CBU} = HMAC(AK, CBU)$

FIGURE 6. **Second phase of RO (Handover Management Step (RO_HO_MAN Step)).**

of these two tools provides more thoroughly and stronger verification while allowing them to complement each other.

A. ANALYSIS WITH BAN LOGIC

For BAN-logic analysis, we focus on only the second step, *i.e.* the RO_HO_MAN step, because it is same as the first one except for the forwarding of RO context and SK_1 or SK_i. In BAN-logic, the basic notations used are shown in Table 2, and the BAN-logic's rules are given below:

Message Meaning Rule (MM):

$$\frac{P \textit{ believes } P \overset{K}{\Leftrightarrow} Q, P \textit{ sees} \langle X\rangle_K}{P \textit{ believes } Q \textit{ said } X}$$

Nonce Verification Rune (NV):

$$\frac{P \textit{ believes } \#(X), P \textit{ believes } Q \textit{ said } X}{P \textit{ believes } Q \textit{ believes } X}$$

Freshness Rule (FR):

$$\frac{P \textit{ believes } \#(X)}{P \textit{ believes } \#(X, Y)}$$

Belief Conjunction Rule (BC):

$$\frac{P \textit{ believes } (X, Y)}{P \textit{ believes } (X)}$$

TABLE 2. **BAN logic statements.**

Statement	Meaning
P believes X	*P* believes *X*, which is treated as true.
P sees X	*P* receives *X* at present or received *X*in the past.
P said X	*P* once said *X*. (*i.e.*, *X* was sent to *P* at some point)
$\#(X)$	*X* is fresh.
$\langle M\rangle_K$	It means that *M* is combined with a secret *K*. HMAC operation can be expressed by this.
$P \overset{K}{\leftrightarrow} Q$	*K* is a secret key only known to *P* and *Q*.
$\overset{K}{\rightarrow} P$	*K* is a *P*'s public key.
$P \overset{K}{\Leftrightarrow} Q$	*K* is a secret only known to *P* and *Q*.

Diffie-Hellman Rule (DH):

$$\frac{P \textit{ believes } Q \textit{ believes } \xrightarrow{g^Y mod\ p} Q, P \textit{ believes } \xrightarrow{g^X mod\ p} P}{P \textit{ believes } P \xleftrightarrow{g^{XY} mod\ p} Q}$$

1) VERIFICATION

BAN-logic has the following three steps for security analysis: (i) translating a protocol into an idealized version (ii) defining assumptions about the initial states (iii) repeatedly applying the above rules until the attainment of aimed beliefs.

a: IDEALIZATION

As the first step, the proposed scheme is idealized as follow:

$$\text{(I1) } nMAG \rightarrow HGW : \left\langle \begin{matrix} ID_{MN}, HNP_{MN}, h(SK_{i-1}), \\ AD_{nMAG}, n^1, ts, \xrightarrow{g^X mod\, p} nMAG \end{matrix} \right\rangle_{SK_i}$$

$$\text{(I2) } HGW \rightarrow nMAG : \left\langle \begin{matrix} ID_{MN}, HNP_{MN}, \\ n_1, n_2 \xrightarrow{g^Y mod\, p} HGW, \\ nMAG \xleftrightarrow{MSK} HGW, MAG_{MSK} \end{matrix} \right\rangle_{SK_i}$$

$$where\ MAG_{MSK}$$

$$= \left\langle \begin{matrix} ID_{MN}, HNP_{MN}, n_1, n_2, h(SK_i), \\ nMAG \xleftrightarrow{EK} HGW, nMAG \xLeftrightarrow{AK} HGW \end{matrix} \right\rangle_{AK}$$

$$\text{(I3) } nMAG \rightarrow HGW : \left\langle \begin{matrix} n_2, nMAG \xleftrightarrow{EK} HGW, \\ nMAG \xLeftrightarrow{AK} HGW \end{matrix} \right\rangle_{AK}$$

Note that only the steps (A) - (E) are skipped because they have no contribution to this analysis.

b: ASSUMPTIONS

In the second step, the following assumptions are made for the initial states.

(A1) $HGW\ believes\ nMAG \xLeftrightarrow{SK_i} HGW$

(A2) $HGW\ believes\ \#\,(ts)$

(A3) $HGW\ believes \xrightarrow{g^Y mod\, p} HGW$

(A4) $HGW\ believes\ \#\,(n_2)$

(A5) $nMAG\ believes\ nMAG \xLeftrightarrow{SK_i} HGW$

(A6) $nMAG\ believes\ \#\,(n_1)$

(A7) $nMAG\ believes \xrightarrow{g^X mod\, p} nMAG$

c: GOALS

The goals of our proposed protocol are defined as shown below. The goals (G1) $\sim$ (G3) are related to mutual authentication while other ones are related to secure key exchange.

(G1) $HGW\ believes\ nMAG\ believes\ ts$

(G2) $HGW\ believes\ nMAG\ believes\ n_2$

(G3) $nMAG\ believes\ HGW\ believes\ n_1$

(G4) $HGW\ believes\ nMAG \xleftrightarrow{MSK} HGW$

(G5) $HGW\ believes\ nMAG \xLeftrightarrow{AK} HGW$

(G6) $HGW\ believes\ nMAG \xleftrightarrow{EK} HGW$

(G7) $nMAG\ believes\ nMAG \xleftrightarrow{MSK} HGW$

(G8) $nMAG\ believes\ nMAG \xLeftrightarrow{AK} HGW$

(G9) $nMAG\ believes\ nMAG \xleftrightarrow{EK} HGW$

(G10) $nMAG\ believes\ HGW\ believes\ nMAG \xLeftrightarrow{AK} HGW$

(G11) $nMAG\ believes\ HGW\ believes\ nMAG \xleftrightarrow{EK} HGW$

(G12) $HGW\ believes\ nMAG\ believes\ nMAG \xLeftrightarrow{AK} HGW$

(G13) $HGW\ believes\ nMAG\ believes\ nMAG \xleftrightarrow{EK} HGW$

d: DERIVATION

With the idealized form and the assumptions, the analyses are executed as follows.

From (I1), we derive:

$$HGW\ sees \left\langle \begin{matrix} ID_{MN}, HNP_{MN}, h(SK_{i-1}), AD_{nMAG}, n_1, \\ ts, \xrightarrow{g^X mod\, p} nMAG \end{matrix} \right\rangle_{SK_i} \quad (1)$$

$$HGW\ believes\ nMAG\ believes \begin{pmatrix} ID_{MN}, HNP_{MN}, \\ h\,(SK_{i-1})\,, \\ AD_{nMAG}, \\ n_1, ts, \\ \xrightarrow{g^X mod\, p} nMAG \end{pmatrix}$$

$$by\ (1)\,, (\mathrm{A1})\,, \mathrm{MM}, (\mathrm{A2})\,, \mathrm{FR}, \mathrm{NV} \quad (2)$$

$$HGW\ believes\ nMAG\ believes \begin{pmatrix} ID_{MN}, HNP_{MN}, \\ AD_{nMAG}, h\,(SK_{i-1}) \end{pmatrix}$$

$$by\ (2)\,, \mathrm{BC} \quad (3)$$

$$HGW\ believes\ nMAG\ believes \xrightarrow{g^X mod\, p} nMAG$$

$$by\ (2)\,, \mathrm{BC} \quad (4)$$

$$HGW\ believes\ nMAG \xleftrightarrow{g^{XY} mod\, p} HGW$$

$$by\ (4)\,, (\mathrm{A3})\,, \mathrm{DH} \quad (5)$$

$$HGW\ believes\ nMAG\ believes\ ts\ by\ (2)\,, \mathrm{BC} \quad (6)$$

$$HGW\ believes\ nMAG \xleftrightarrow{MSK} HGW$$

$$by\ (2)\,, BC, (6)\,, (\mathrm{A4})\,, (5) \quad (7)$$

$$HGW\ believes\ nMAG \xLeftrightarrow{AK} HGW\ by\ (7) \quad (8)$$

$$HGW\ believes\ nMAG \xleftrightarrow{EK} HGW\ by\ (7) \quad (9)$$

From (I2), we derive:

$$nMAG\ sees \left\langle \begin{matrix} ID_{MN}, HNP_{MN}, n_1, n_2 \xrightarrow{g^Y mod\, p} HGW, \\ nMAG \xleftrightarrow{MSK} HGW, MAG_{MSK} \end{matrix} \right\rangle_{SK_i}$$

$$(10)$$

$$nMAG\ believes\ HGW\ believes$$

$$\times \begin{pmatrix} ID_{MN}, HNP_{MN}, n_1, n_2, \xrightarrow{g^Y mod\, p} HGW, \\ nMAG \xleftrightarrow{MSK} HGW, MAG_{MSK} \end{pmatrix}$$

$$by\ (10)\,, (\mathrm{A5})\,, \mathrm{MM}, (\mathrm{A6})\,, \mathrm{FR}, \mathrm{NV} \quad (11)$$

$$nMAG\ believes\ HGW\ believes\ \mathrm{n}_2\ by\ (11)\,, \mathrm{BC} \quad (12)$$

$$nMAG\ believes\ HGW\ believes \xrightarrow{g^Y mod\, p} HGW$$

$$by\ (11)\,, \mathrm{BC} \quad (13)$$

$$nMAG\ believes\ nMAG \xleftrightarrow{g^{XY} mod\, p} HGW$$

$$by\ (13)\,, (\mathrm{A7})\,, \mathrm{DH} \quad (14)$$

$$nMAG\ believes\ HGW\ believes\ \mathrm{n}_2\ by\ (11)\,, \mathrm{BC} \quad (15)$$

$$nMAG\ believes\ nMAG \xleftrightarrow{MSK} HGW$$

$$by\ (15)\,, (\mathrm{A6})\,, (14) \quad (16)$$

$$nMAG\ believes\ nMAG \xLeftrightarrow{AK} HGW\ by\ (16) \quad (17)$$

$$nMAG\ believes\ nMAG \xleftrightarrow{EK} HGW\ by\ (16) \quad (18)$$

$$nMAG\ sees \left\langle \begin{matrix} ID_{MN}, HNP_{MN}, n_1, n_2, h(SK_i), \\ nMAG \xleftrightarrow{EK} HGW, nMAG \overset{AK}{\Longleftrightarrow} HGW \end{matrix} \right\rangle_{AK}$$
$$by\ \ (11)\,,\mathrm{BC} \qquad (19)$$

$$nMAG\ believes\ HGW\ believes$$
$$\times \left(\begin{matrix} ID_{MN}, HNP_{MN}, n_1, \\ n_2, h\,(SK_i)\,, nMAG \xleftrightarrow{EK} HGW, nMAG \overset{AK}{\Longleftrightarrow} HGW \end{matrix} \right)$$
$$by\ \ (19)\,, (17)\,, \mathrm{MM},\ (\mathrm{A6})\,, \mathrm{FR},\ \mathrm{NV} \qquad (20)$$

$$nMAG\ believes\ HGW\ believes\ nMAG \xleftrightarrow{EK} HGW$$
$$by\ \ (20)\,, \mathrm{BC} \qquad (21)$$

$$nMAG\ believes\ HGW\ believes\ nMAG \overset{AK}{\Longleftrightarrow} HGW$$
$$by\ \ (20)\,, \mathrm{BC} \qquad (22)$$

From (I3), we derive:

$$HGW\ sees\ \langle n_2, nMAG \xleftrightarrow{EK} HGW, nMAG \overset{AK}{\Longleftrightarrow} HGW \rangle_{AK} \qquad (23)$$

$$HGW\ believes\ nMAG\ believes$$
$$\times \left(n_2, nMAG \xleftrightarrow{EK} HGW, nMAG \overset{AK}{\Longleftrightarrow} HGW \right)$$
$$by\ \ (23)\,, (8)\,, \mathrm{MM},\ (\mathrm{A4}),\ \mathrm{FR},\ \mathrm{NV} \qquad (24)$$

$$HGW\ believes\ nMAG\ believes\ nMAG \xleftrightarrow{EK} HGW$$
$$by\ \ (24)\,, \mathrm{BC} \qquad (25)$$

$$HGW\ believes\ nMAG\ believes\ nMAG \overset{AK}{\Longleftrightarrow} HGW$$
$$by\ \ (24)\,, \mathrm{BC} \qquad (26)$$

$$HGW\ believes\ nMAG\ believes\ n_2\ \mathrm{by}\ \ (24)\,, \mathrm{BC} \qquad (27)$$

From the above analysis, it is shown that the goals (G1), (G2), and (G3) are achieved through the obtained beliefs (6), (15), and (27). In addition, the goals (G4) $\sim$ (G9) are satisfied with the beliefs (7) $\sim$ (9) and (16) $\sim$ (18) while the rest are satisfied with the beliefs (21), (22), (25), and (25). In summary, the proposed protocol achieves all the goals.

2) SECURITY PROPERTIES

Lemma 1: HGW and nMAG mutually authenticate each other.

Proof: The derived belief (27) enables an HGW to confirm that the correspondent nMAG believes its messages. More importantly, we can derive the following belief (28) by applying BC to (2):

$$HGW\ believes\ nMAG\ believes\ h\,(SK_{i-1}) \qquad (28)$$

that can prevent a malicious MAG from lying that a victim *MN* arrives at its network because it cannot know $h\,(SK_{i-1})$ without the pMAG's support. Therefore, it is enough to say that the HGW authenticates the nMAG because it believes the authenticity of the nMAG's last message. On the other hand, it is shown from the obtained belief (15) that the nMAG authenticates the HGW because it trusts the authenticity of the HGW's message. As a result, it is concluded that the HGW and the nMAG mutually authenticates each other. □

Lemma 2: The session keys *EK* and *AK* are securely exchanged between HGW and nMAG.

Proof: While believing the session keys *EK* and *AK* based on the beliefs (8) and (9), an HGW can confirm that the correspondent nMAG believes those keys through the beliefs (25) and (26).That makes it possible for the HGW to trust that the two keys are safe to use. Similarly, the nMAG can arrive at the conclusion that the session keys are securely shared with the HGW through the beliefs (17), (18), (21), and (22). Consequently, we can conclude that the session keys *EK* and *AK* are securely exchanged between the HGW and the nMAG. □

Lemma 3: Perfect Forward Secrecy (PFS) is guaranteed.

Proof: It is assumed that *EK* is used to encrypt the messages exchanged between the MN and its CN. One of our aims is to achieve *PFS* by preventing the encrypted messages transmitted in the previous sessions from being recovered to their original form even when the long-term key, $K_{LMA-HGW}$, is compromised or the current session keys (or the successive ones), *MSK* and*EK*, are compromised. The derived beliefs (5), (7), (14), and (16) demonstrate that *MSK* is securely exchanged based on the Diffie-Hellman key exchange. Moreover, in every session, the two entities randomly generate and temporarily use their private keys, which are then discarded. Thus, the private keys cannot be recovered after their session finishes even in the case of the compromise for the above key. Note that, as indicated in the beliefs (9) and (18), *EK* is derived from *MSK*, and thus, follows its security. Therefore, we can confirm that the proposed protocol satisfies PFS. □

Lemma 4: The MNs' privacy is kept in the MAG-HGW path.

Proof: The messages EBU, EBA, and CBU which are transmitted between the associated MAG and HGW don't include the values, ID_{MN} and HNP_{MN}, which can identify MNs. Instead, they are just involved to compute the message authentication codes, MAG_{EBU}, MAG_{EBA}, MAG_{MSK} as well as the session key SK_1 or SK_{i}. Thus, upon receiving the EBU message, a HGW should find a MN with its all MNs' ID_{MN} and HNP_{MN}. As a result, we can say that the proposed protocol keeps the MNs' privacy in the MAG-HGW path. □

Lemma 5: The proposed protocol is secure against the resource exhaustion attacks.

Proof: In the proposed protocol, an HGW first tries to arrive at the belief (5) by verifying the given MAG_{EBU} prior to its expensive public key operations. In this way, it can avoid to suffer from a storm of public key operations caused by resource exhaustion attacks. Similarly, the MAG or nMAG first verifies MAG_{EBA}, and then executes the successive public key operations. Consequently, it is clear that the proposed protocol is secure against the resource exhaustion attacks. □

Lemma 6: The proposed protocol is secure against the redirection attacks by a malicious MAG.

Proof: Most of all let us consider the first step, *i.e.*, the RO_INIT step. In this phase, without receiving the RO-INIT message from the LMA, a malicious MAG cannot launch the redirection attacks because it does not know SK_1. Note that

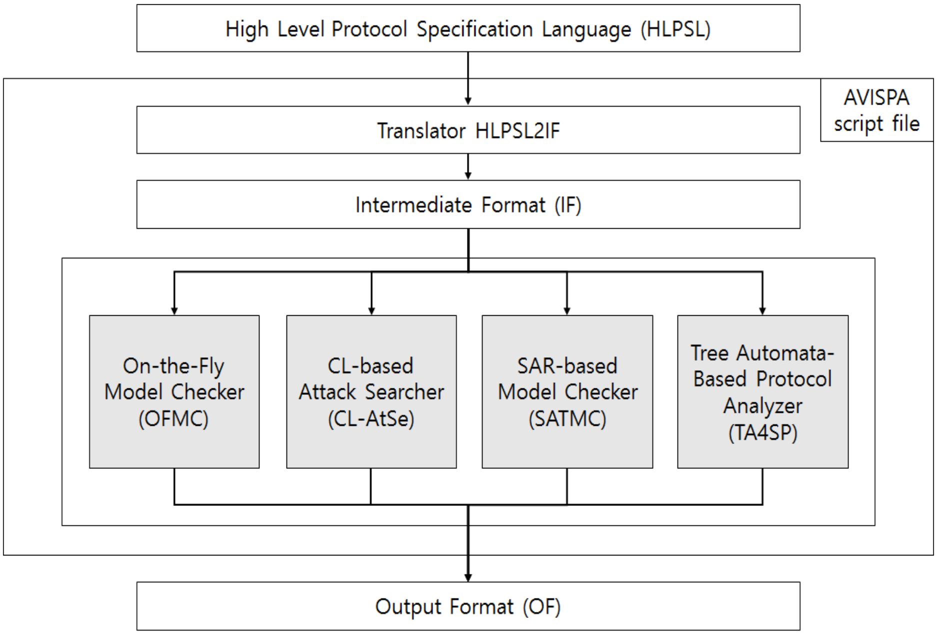

High Level Protocol Specification Language (HLPSL)
AVISPA script file
Translator HLPSL2IF
Intermediate Format (IF)
On-the-Fly Model Checker (OFMC)
CL-based Attack Searcher (CL-AtSe)
SAR-based Model Checker (SATMC)
Tree Automata-Based Protocol Analyzer (TA4SP)
Output Format (OF)

FIGURE 7. Architecture of AVISPA.

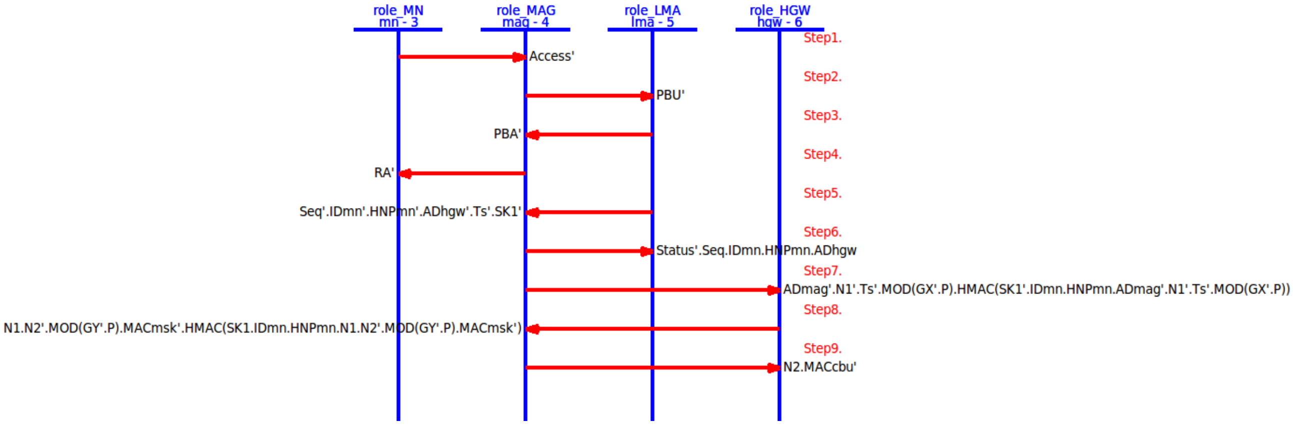

role_MN
mn - 3
role_MAG
mag - 4
role_LMA
lma - 5
role_HGW
hgw - 6
Step1.
Access'
Step2.
PBU'
Step3.
PBA'
Step4.
RA'
Step5.
Seq'.IDmn'.HNPmn'.ADhgw'.Ts'.SK1'
Step6.
Status'.Seq.IDmn.HNPmn.ADhgw
Step7.
ADmag'.N1'.Ts'.MOD(GX'.P).HMAC(SK1'.IDmn.HNPmn.ADmag'.N1'.Ts'.MOD(GX'.P))
Step8.
N1.N2'.MOD(GY'.P).MACmsk'.HMAC(SK1.IDmn.HNPmn.N1.N2'.MOD(GY'.P).MACmsk')
Step9.
N2.MACcbu'

FIGURE 8. Flow of RO-INIT step.

the HGW sends the RO-INIT message to MAG only when RO decision is made. On the other hand, in the RO_HO_MAN phase, nMAG has to receive the HO_CTX message from pMAG to send the EBU message. Clearly, it is impossible for a malicious MAG to launch the redirection attacks because it should deceive pMAG into believing an MN handovers to itself. □

B. ANALYSIS WITH AVISPA

AVISPA is an automated tool used for formal verification, which provides functions for specification, verification, analysis, presentation, and derivation about protocols and applications [69]. AVISPA uses the High-Level Protocol Specification Language (HLPSL) to model a protocol. AVISPA converts the protocol specification written in HLPSL into Intermediate Format (IF) through HLPSL2IF. The transformed specification derives its results through 4 sub-modules, namely, On-the-Fly Model-Checker (OFMC), Constraint-Logic-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC), and Automatic Approximations for the Analysis of Security Protocols (TA4SP).

Fig. 7 presents the operational architecture of AVISPA. The proposed RO protocol is divided the RO_INIT and RO_HO_MAN steps, each of which is modeled in HLPSL and verified through AVISPA. The simulated flows of the two modeled steps are shown in Figs. 8 and 9. Figures 10 and 11 demonstrate the OFMC and CL-AtSe results for the RO_INIT step while Figs. 12 and 13 show those of the RO_HO_MAN step. These results correspond to the theoretical analysis, and prove that the proposed RO protocol is safe to attacks.

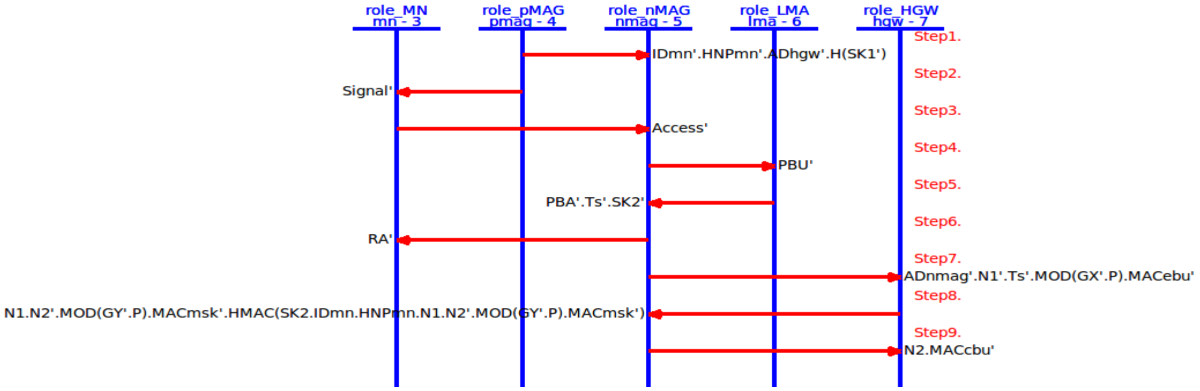
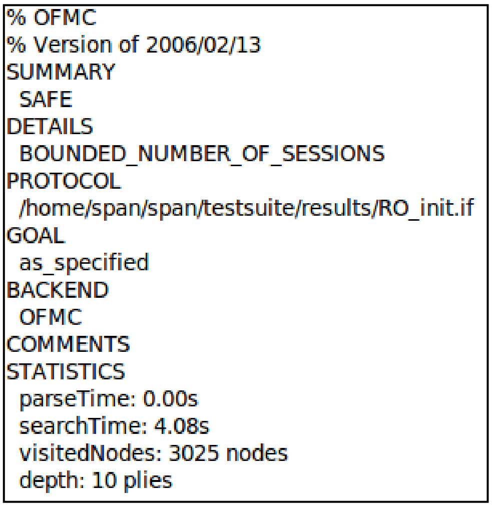
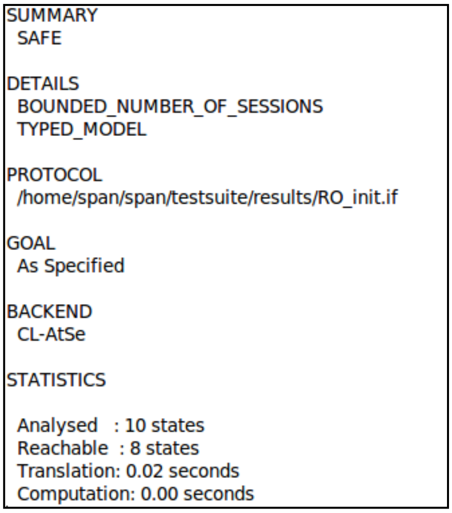


FIGURE 9. Flow of RO-HO-MAN step.



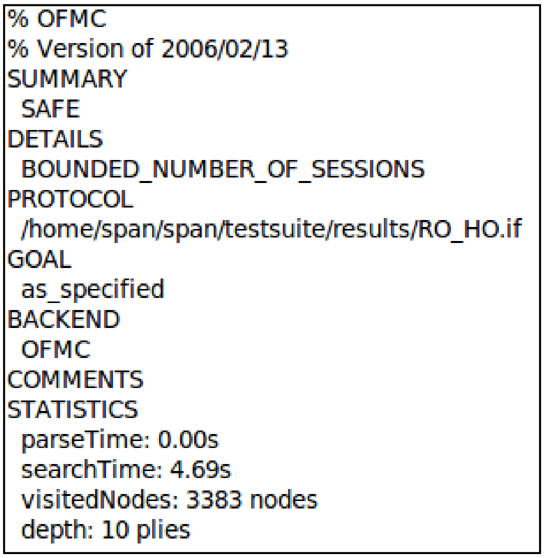
```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/RO_init.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 4.08s
  visitedNodes: 3025 nodes
  depth: 10 plies
```

FIGURE 10. The output of OFMC back-end (RO-INIT step).



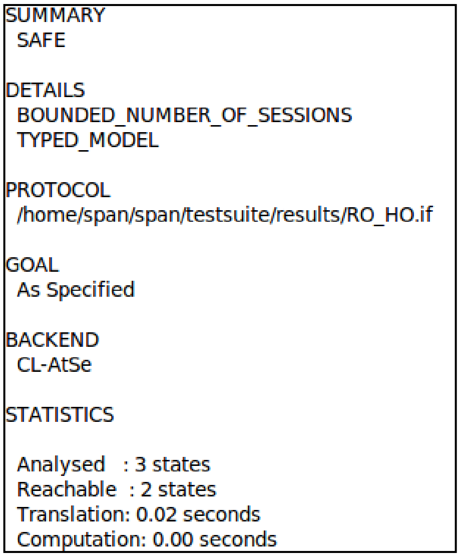
```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

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

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 10 states
  Reachable  : 8 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

FIGURE 11. The output of CL-AtSe back-end (RO-INIT step).



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/RO_HO.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 4.69s
  visitedNodes: 3383 nodes
  depth: 10 plies
```

FIGURE 12. The output of OFMC back-end (RO-HO-MAN step).



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

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

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 3 states
  Reachable  : 2 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

FIGURE 13. The output of CL-AtSe back-end (RO-HO-MAN step).

V. PERFORMANCE EVALUATION

The proposed secure RO approach is evaluated for its performance by using NS-2 [67]. The proposed approach is evaluated in two scenarios, the first one comprising flow through via LMA, which is a default case and the second is optimized routing using the LMA only in the initial phase. The simulations are conducted using a total of 50 sensors (CN) in a smart house IoT network as shown in Fig 14. Each

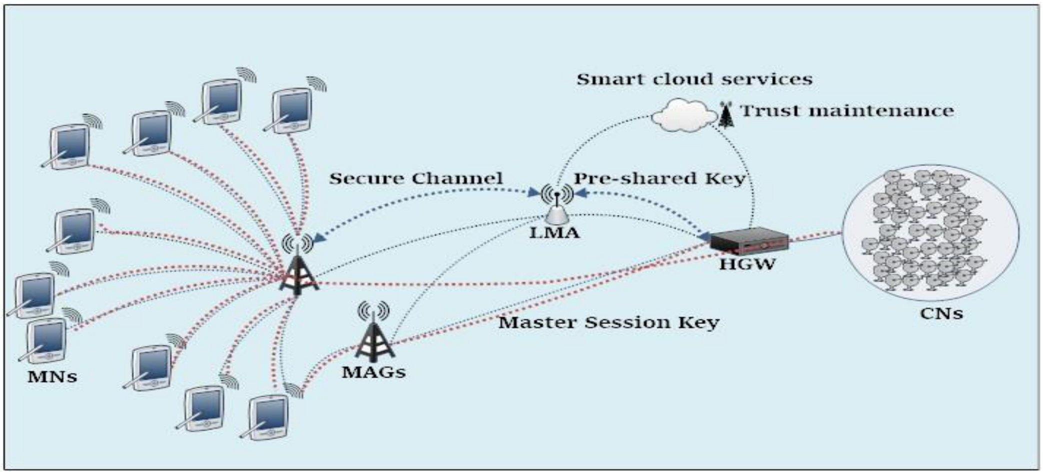


FIGURE 14. An illustration of the simulation scenario considered for evaluation of the proposed approach.

TABLE 3. Simulation configurations.

Parameter	Value
Area	1000 x 1000 sq.m.
MN	100-500
CN	50
MAG	2
HGW	1
LMA	1
Agent	TCP-New Reno
MAC	802.11
Radio Propagation	Two Ray Ground
Distance	50m-150m
Data	625 Mb
Initial data	0.125 Mb
Antenna	Omni Antenna
Channel	Wireless Channel
Max. Speed	20 kmph
Min. Speed	10 kmph
Simulation Time	100 s
Simulation Runs	50

of the sensors serves as an equipment controller. A single HGW is created to manage these sensors. It is assumed that the trust is established between the LMA and HGW during the start of the simulations. Multiple MAGs are created on the side of MNs that move using random waypoint model. TCP-NewReno is used as an agent to provide TCP traffic link between the CNs and HGW as it is capable of providing fast recovery and retransmissions. A total of 50 simulation runs is performed and the results are observed for average values. Results are evaluated for handover latency, end to end delay, throughput, transmission rate during handovers and packet loss. The parameters used to evaluate the proposed approach are presented in Table 3.

A. HANDOVER LATENCY

Handover latency is the measure of time consumed after the initiation of the handovers and its completion. Handover latency provides evaluation regarding the speed of a network in connecting an MN to the new MAG. In the proposed approach, MN moves between MAGs and handover takes place every time the MN moves towards the new MAG. The simulation results show that the proposed approach provides a steady latency, which remains same despite the number of MNs in a network. But, with variation in the number of nodes, the handover latency is affected and increases with an increase in the number of MNs, as shown in Fig. 15. This latency can be further controlled by optimizing the bandwidth of a network. The results show that the proposed approach provides 38.7% lesser handover latency than the default scenario operating without RO. The maximum latency recorded for the proposed approach is 10.1 ms, whereas for the default scenario, the maximum value is 15.8 ms. With lower handover latency, it is evident that the proposed approach provides security without compromising the mobility of MNs.

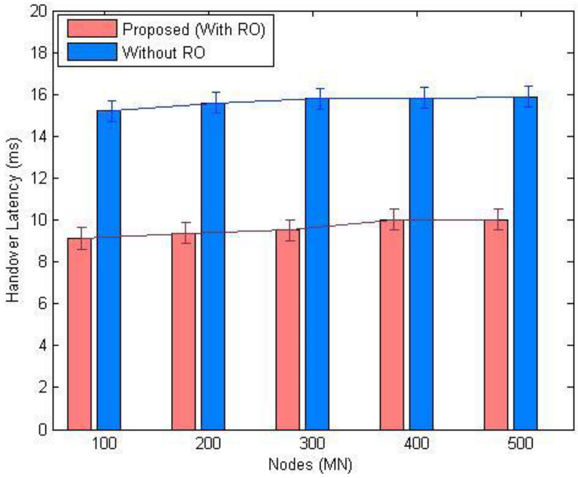


FIGURE 15. Handover latency vs. nodes.

B. END TO END DELAY (E2E)

E2E is the measure of the delays induced before the initiation and after the completion of the handovers. It accounts for transmission, propagation, queuing, and processing delays. A network with lower E2E provides better connectivity and can handle sensitive traffic, such as multimedia traffic, efficiently. The continuity of traffic over the network using a bypassing methodology over the LMA allows 15.1% lesser delays in the proposed approach as compared to the default case, as shown in Fig. 16.

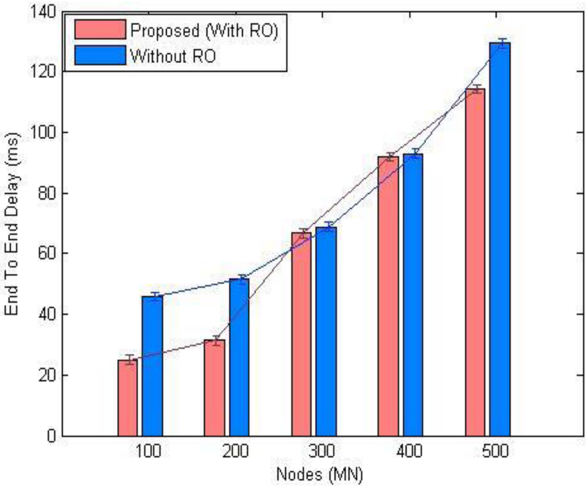


FIGURE 16. End to End Delay vs. nodes.

The result shows that the variation in delays is affected by the variation in the number of MNs. Further, with a large value of link delay and a higher number of MNs, the E2E delay increases, but this increase is well in control allowing the network to perform efficiently even in a scenario with limited support from the underlying network.

C. NETWORK THROUGHPUT

Network throughput is the measure of the overall transmission speed attained in the network. It provides analyses of the number of bits transferred per second in the network during entire session of connectivity. The network throughput is recorded against the variation in the number of nodes over a consistent traffic without altering the data and the initial rate of transmission. Fig. 17 presents the throughput comparison of the proposed RO strategy and a default case without RO. The results show that the proposed approach, despite the variation in security methodology, provides 18.18% better throughput during the entire session of transmission. The results show that the proposed approach provides a highest of 36.006 Mbps (or 38000.6 Kbps) whereas the default scenario could sustain a highest of 31.00 Mbps (or 31000.6 Kbps) in a network with only 100 MNs.

However, the adverse case provides lesser throughput as a large number of MNs make connections simultaneously with the same CNs, which is an almost impossible scenario to occur in a real time. Thus, considering the average number of users, the proposed approach is capable of providing high throughput during the entire session of connectivity.

D. TRANSMISSION RATE DURING HANDOVERS

With provisioning of security enhancement and RO by overcoming the excessive transmission via LMA, the proposed approach provides early binding, which allows high traffic transmission even during the handover scenarios. The results for transmission rate during the handovers are shown in Fig. 18. The results show that the proposed scenario is capable of providing 63.1% higher transmission rate during the handovers in comparison with a scenario which uses the LMA for every pass. With sufficient rate even during the handovers, the proposed approach allows better connectivity and can be used to further incorporate heavy security operations in flow between the MNs and CNs.

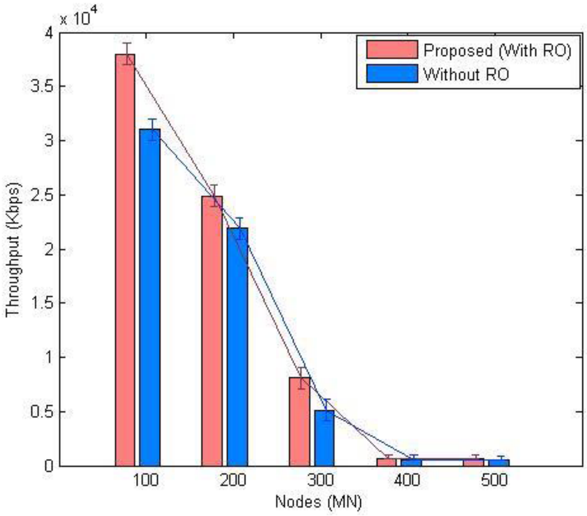


FIGURE 17. Network Throughput vs. nodes.

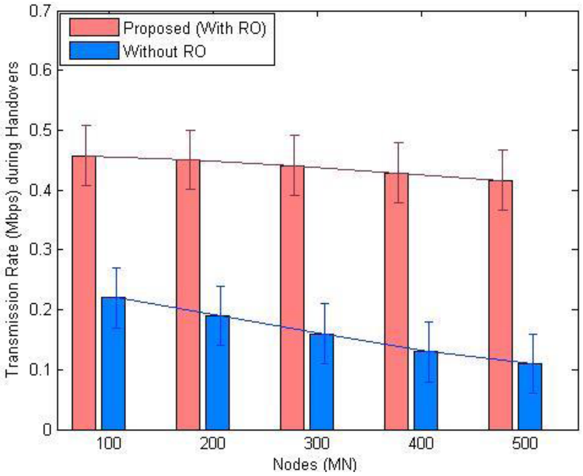


FIGURE 18. Transmission rate during handovers vs. nodes.

E. PACKET LOSS

The proposed approach provides better transmission support to entire network and removes the excessive overheads of transmission via LMA even after authentication. This allows more traffic to pass efficiently without much delay and loss. With lesser delay, even with minimum support from the underlying channel and increasing number of users,

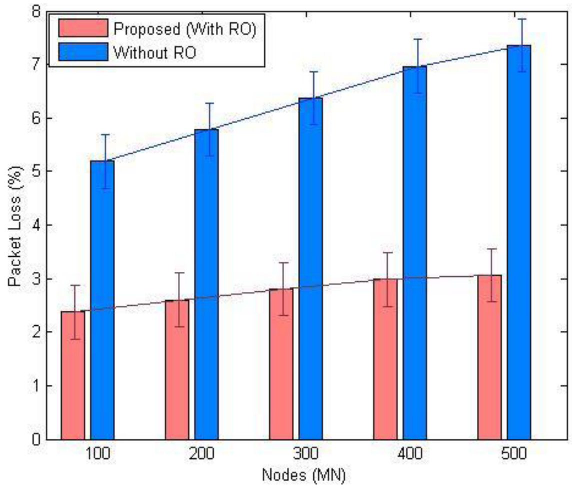


FIGURE 19. Packet loss vs. nodes.

the proposed approach provides higher delivery support and less packet loss as shown in Fig. 19.The results show that the proposed approach provides 2.3% loss in the overall traffic at the minimum support from the link, which is 56.3% lower than the default scenario. The results shown in terms of packet loss suggest that the proposed approach is capable of providing higher delivery rate with sufficiently high transmission speed.

VI. CONCLUSION

In this paper, the problem of efficient communication in SH-IoT networks was considered in the form of RO, and a secure protocol was proposed, which used PMIPv6 domain divisibility to ensure the security as well as performance over the path between the MN and the CN. The proposed protocol used the pre-established trust relationship between the MN's HGW and the PMIPv6 domain (i.e., LMA), where the session keys exchange was performed on the basis of Diffie-Hellman security algorithm. The correctness of the proposed protocol was formally and precisely analyzed using BAN-logic and AVISPA. Further, network simulations were conducted to evaluate the performance of the proposed protocol. The results showed that the proposed approach was capable of providing secure transmission by overcoming the RO problem in PMIPv6 along with a reduction in handover latency, end to end delay, and packet loss. The proposed approach provided high throughput and transmission rate during the handover phase in comparison with a smart home network operating with the default PMIPv6. The results showed that the proposed approach provided 38.7% lower handover latency, 15.1% lesser end to end delays, 56.3% lower packet loss, 18.18% higher throughput, and 63.1% higher transmission rate during handover phase in comparison with SH-IoT network operating with the default PMIPv6.

In future, the proposed protocol will be extended to consider *distributed mobility management* with 5G while trust-reestablishment and performance will be evaluated using varying traffic and mobility models.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

SUPPLEMENTARY FILES

The results and codes for AVISPA are provided as separate files available at http://ieeexplore.ieee.org..

REFERENCES

[1] A. C. Jose, R. Malekian, and N. Ye, "Improving home automation security; integrating device fingerprinting into smart home," *IEEE Access*, vol. 4, pp. 5776–5787, 2016.

[2] Z. W. Kennedy *et al.*, "Home security system with automatic context-sensitive transition to different modes," U.S. Patent 9 501 924 B2, Nov. 22, 2016.

[3] K. Islam, W. Shen, and X. Wang, "Security and privacy considerations for wireless sensor networks in smart home environments," in *Proc. IEEE 16th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2012, pp. 626–633.

[4] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and secure session-key establishment scheme in smart home environments," *IEEE Sensors J.*, vol. 16, no. 1, pp. 254–264, Jan. 2016.

[5] S. Peter and R. K. Gopal, "Multi-level authentication system for smart home-security analysis and implementation," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, vol. 2. Aug. 2016, pp. 1–7.

[6] W. M. S. Stout and V. E. Urias, "Challenges to securing the Internet of Things," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2016, pp. 1–8.

[7] 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.

[8] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 636–654.

[9] Y. Wang, Y. Zhao, S. Jiang, H. Feng, F. Li, and J. Wang, "Design of the smart-home security system based on cloud computing," in *Proc. Int. Conf. Inform. Eng. Commun. Technol. (IECT), China, Proc. DEStech Trans. Eng. Technol. Res.*, pp. 1–7, doi: 10.12783/dtetr/iect2016/3714.

[10] S. Madakam, and H. Date, "Security mechanisms for connectivity of smart devices in the Internet of Things," in *Connectivity Frameworks for Smart Devices*. Cham, Switzerland: Springer, 2016, pp. 23–41.

[11] 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. (SSIC)*, Aug. 2015, pp. 1–6.

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

[13] A. Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 727–732.

[14] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the Internet of Things," *J. Netw. Comput. Appl.*, vol. 83, pp. 12–27, Apr. 2017.

[15] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Aug. 2016, pp. 147–156.

[16] F. E. Fernandes, G. Yang, H. M. Do, and W. Sheng, "Detection of privacy-sensitive situations for social robots in smart homes," in *Proc. IEEE Int. Conf. Autom. Sci. Eng. (CASE)*, Aug. 2016, pp. 727–732.

[17] C. E. Perkins, "Securing mobile IPv6 route optimization using a static shared key," Internet Soc., USA, Tech. Rep. 4449, 2006.

[18] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," Internet Soc., USA, Tech. Rep. 3775, 2004.

[19] A. K. Barbudhe, V. K. Barbudhe, and C. Dhawale, "Comparative analysis of security mechanism of mobile IPv6 threats against binding update, Route Optimization and Tunneling," in *Proc. IEEE 6th Int. Conf. Adapt. Sci. Technol. (ICAST)*, Oct. 2014, pp. 1–7.

[20] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, and R. H. Deng, "Routing optimization security in mobile IPv6," *Comput. Netw.*, vol. 50, no. 13, pp. 2401–2419, Sep. 2006.

[21] D. Kavitha, K. E. S. Murthy, and S. Z. ul Huq, "Security analysis of binding update protocols in route optimization of MIPv6," in *Proc. Int. Conf. Recent Trends Inf. Telecommun. Comput. (ITC)*, Mar. 2010, pp. 44–49.

[22] S. Song, H.-K. Choi, and J.-Y. Kim, "A secure and lightweight approach for routing optimization in mobile IPv6," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, p. 957690, Dec. 2009.

[23] F. Al Hawi, C. Y. Yeun, and K. Salah, "Secure framework for the return routability procedure in MIPv6," in *Proc. IEEE Int. Conf. IEEE Cyber, Phys. Soc. Comput. Green Comput. Commun. (GreenCom)*, Aug. 2013, pp. 1386–1391.

[24] A. Mehdizadeh, S. Khatun, B. M. Ali, R. S. A. R. Abdullah, and G. Kurup, "Secured route optimization in mobile IPv6 wireless networks in terms of data integrity," in *Proc. Int. Conf. Comput. Commun. Eng. (ICCCE)*, May 2008, pp. 643–646.

[25] A. Mehdizadeh, S. Khatun, B. M. Ali, R. S. A. R. Abdullah, and G. Kurup, "Route optimization security in mobile IPv6 wireless networks: A test-bed experience," in *Advances in Computer Science and Engineering*. Berlin, Germany: Springer, 2008, pp. 153–159.

[26] A. Rossi, S. Pierre, and S. Krishnan, "Secure route optimization for MIPv6 using enhanced CGA and DNSSEC," *IEEE Syst. J.*, vol. 7, no. 3, pp. 351–362, Sep. 2013.

[27] A. A. Diana, V. Ragavinodhini, K. Sundarakantham, and S. M. Shalinie, "SHAD: Swift home agent discovery mechanism to mitigate home registration latency in MIPv6 network," *Int. Inf. Inst. Inf.*, vol. 17, no. 4, pp. 1375–1381, 2014.

[28] S. Taha and X. (Sherman) Shen, "ALPP: Anonymous and location privacy preserving scheme for mobile IPv6 heterogeneous networks," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 401–419, 2013.

[29] I. You, "A ticket based binding update authentication method for trusted nodes in mobile IPv6 domain," in *Proc. Int. Conf. Embedded Ubiquitous Comput.*, 2007, pp. 808–819.

[30] 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, 2010.

[31] J.-M. Lee, J.-H. Lee, and T.-M. Chung, "Performance analysis of route optimization on proxy mobile IPv6," in *Proc. 3rd Int. Conf. Syst. Netw. Commun. (ICSNC)*, 2008, pp. 280–285.

[32] J. Guan, I. You, C. Xu, H. Zhou, and H. Zhang, "Survey on route optimization schemes for proxy mobile IPv6," in *Proc. 6th Int. Conf. Innov. Mobile Internet Ser. Ubiquitous Comput. (IMIS)*, Jul. 2012, pp. 541–546.

[33] S. M. Raza, P. Thorat, R. Challa, H. Choo, D. S. Kim, "SDN based inter-domain mobility for PMIPv6 with route optimization," in *Proc. IEEE NetSoft Conf. Workshops (NetSoft)*, Jun. 2016, pp. 24–27.

[34] P. Kim, S. Kim, J. Jin, and S. Lee, "Proactive correspondent registration for Proxy Mobile IPv6 route optimization," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 11, pp. 149–155, 2007.

[35] F.-Y. Leu, C.-Y. Liu, J.-C. Liu, F.-C. Jiang, and H. Susanto, "S-PMIPv6: An intra-LMA model for IPv6 mobility," *J. Netw. Comput. Appl.*, vol. 58, pp. 180–191, Dec. 2015.

[36] B.-J. Han, J.-M. Lee, J.-H. Lee, and T.-M. Chung, "PMIPv6 route optimization mechanism using the routing table of MAG," in *Proc. 3rd Int. Conf. Syst. Netw. Commun. (ICSNC)*, 2008, pp. 274–279.

[37] T. Chiba, H. Yokota, A. Dutta, D. Chee, and H. Schulzrinne, "Route optimization for proxy mobile IPv6 in IMS network," in *Proc. 2nd Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2008, pp. 1–9.

[38] Y.-H. Choi and T.-M. Chung, "Using correspondent information for route optimization scheme on Proxy Mobile IPv6," *JNW*, vol. 5, no. 8, pp. 984–989, Aug. 2010.

[39] B. Kang, N. Kwon, and H. Choo, "Developing route optimization-based PMIPv6 testbed for reliable packet transmission," *IEEE Access*, vol. 4, pp. 1039–1049, 2016.

[40] Y. Wang, Y. Feng, and L. Zhang, "Coordinating fast handover and route optimization in proxy mobile IPv6," in *Proc. 5th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCom)*, Sep. 2009, pp. 1–4.

[41] M.-C. Chuang, J.-F. Lee, and M.-C. Chen, "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," *IEEE Syst. J.*, vol. 7, no. 1, pp. 102–113, Mar. 2013.

[42] S. H. Hwang, J. H. Kim, C. S. Hong, and J.-S. Sung, "Localized management for proxy mobile IPv6," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, 2010, pp. 1–5.

[43] P. A. R. K. Sihun, K. A. N. G. Namhi, and K. I. M. Younghan, "Localized proxy-MIPv6 with route optimization in IP-based networks," *IEICE Trans. Commun.*, vol. 90, no. 12, pp. 3682–3686, 2007.

[44] A. Rasem, M. St-Hilaire, and C. Makaya, "Efficient handover with optimized localized routing for Proxy Mobile IPv6," *Telecommun. Syst.*, vol. 62, no. 4, pp. 675–693, 2016.

[45] A. Rasem, C. Makaya, and M. St-Hilaire, "O-PMIPv6: Efficient handover with route optimization in proxy mobile IPv6 domain," in *Proc. 8th IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2012, pp. 47–54.

[46] C. Cho, J.-Y. Choi, J. Jeong, and T.-M. Chung, "Performance analysis of inter-domain handoff scheme based on virtual layer in PMIPv6 networks for IP-based Internet of Things," *PloS One*, vol. 12, no. 1, p. e0170566, 2017.

[47] J. Guan, H. Zhou, Z. Yan, Y. Qin, and H. Zhang, "Implementation and analysis of proxy MIPv6," *Wireless Commun. Mobile Comput.*, vol. 11, no. 4, pp. 477–490, 2011.

[48] A. J. Jabir, S. Shamala, Z. Zuriati, and N. Hamid, "A comprehensive survey of the current trends and extensions for the proxy mobile IPv6 protocol," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2015.2497146.

[49] H. Modares, A. Moravejosharieh, J. Lloret, and R. B. Salleh, "A survey on Proxy Mobile IPv6 handover," *IEEE Syst. J.*, vol. 10, no. 1, pp. 208–217, Mar. 2016.

[50] S. E. O. Won-Kyeong, L. E. E. Kang-Won, C. H. O. I. Jae-In, and C. H. O. You-Ze, "An efficient route optimization scheme for multiple LMAs in PMIPv6 domain," *IEICE Trans. Commun.*, vol. 95, no. 10, pp. 3149–3157, 2012.

[51] K.-S. Kong, "A PMIPv6-based auxiliary mobility management considering traffic locality," in *Proc. Int. Conf. Comput. Sci. Appl.*, 2016, pp. 1053–1058.

[52] J. Baek, "Secure pre-authentication schemes for fast handoff in Proxy Mobile IPv6," *J. Inf. Commun. Converg. Eng.*, vol. 14, no. 2, pp. 89–96, 2016.

[53] L. A. Magagula and H. A. Chan, "Early discovery and pre-authentication in Proxy MIPv6 for reducing handover delay," in *Proc. 3rd Int. Conf. Broadband Commun., Inf. Technol. Biomed. Appl.*, 2008, pp. 280–285.

[54] A. K. Tripathi, R. Radhakrishnan, and J. S. Lather, "Optimized and secure authentication Proxy Mobile IPv6 (OS-PMIPv6) scheme for reducing packet loss," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 6, pp. 510–515, 2016.

[55] T. Gao, L. Tan, P. Qiao, and K. Yim, "An access authentication scheme based on hierarchical IBS for Proxy Mobile IPV6 network," *Intell. Auto. Soft Comput.*, vol. 22, no. 3, pp. 389–396, 2016.

[56] I. You, J. D. Lim, J. N. Kim, H. Ahn, and C. Choi, "Adaptive authentication scheme for mobile devices in Proxy MIPv6 networks," *IET Commun.*, vol. 10, no. 17, pp. 2319–2327, 2016.

[57] M. Liebsch and S. Jeong, "Proxy mobile IPv6 (PMIPv6) localized routing problem statement," IETF USA, Tech. Rep. 6279, 2011.

[58] Q. Wu and J. Korhonen, "Problem statement of IPv4 support for PMIPv6 localized routing," IETF Draft, Draft: draft-wu-netext-pmipv6-ipv4-ro-ps-01, 2009. [Online]. Available: https://tools.ietf.org/html/draft-wu-netext-pmipv6-ipv4-ro-ps-01

[59] S. Krishnan, R. Koodli, P. Loureiro, Q. Wu, and A. Dutta, "Localized routing for proxy mobile IPv6," RFC, USA, Tech. Rep. 6705. 2012.

[60] S. Kent, "IP encapsulating security payload (ESP)," Internet Soc., USA, Tech. Rep. 4303, 2005. [Online]. Available: https://www.ietf.org/rfc/rfc4303.txt

[61] S. Gundavelli, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," IETF RFC, USA, Tech. Rep. 5213, Aug. 2008, p. 93. [Online]. Available: https://tools.ietf.org/html/rfc5213

[62] "Resource exhaustion attack," accessed on Mar. 8, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Resource_exhaustion_attack

[63] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Philos. Trans. Roy. Soc. Lond. A, Math. Phys. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.

[64] I. You, Y. Hori, and K. Sakurai, "Enhancing SVO logic for mobile IPv6 security protocols," *JoWUA*, vol. 2, no. 3, pp. 26–52, 2011.

[65] I. You, Y. Hori, and K. Sakurai, "Towards formal analysis of wireless LAN security with MIS protocol," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 7, no. 2, pp. 112–120, 2011.

[66] You, Ilsun, and Fang-Yie Leu, "Comments on 'SPAM: A secure password authentication mechanism for seamless handover in Proxy Mobile IPv6 networks,'" *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2015.2477415

[67] T. Issariyakul and E. Hossain. *Introduction to Network Simulator NS2*. New York, NY, USA: Springer, 2011.

[68] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1997.

[69] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, May 2006.

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

VISHAL SHARMA received the B.Tech. degree in computer science and engineering from Punjab Technical University in 2012 and the Ph.D. degree in computer science and engineering from Thapar University in 2016. He was with Thapar University as a Lecturer in 2016. He is currently a Post-Doctoral Researcher with the MobiSec Laboratory, Department of Information Security Engineering, Soonchunhyang University, Asan, South Korea. His areas of research and interests are 5G networks, UAVs, estimation theory, and artificial intelligence. He is a member of various professional bodies and the past Chair of the ACM Student Chapter-Patiala.

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

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

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 Chairperson of the Department of Information Security Engineering, Soonchunhyang University, Asan, South Korea. His main research interests include Internet security, authentication, access control, and formal security analysis. He is a Fellow of the IET. He has served or is currently serving as a main organizer of international conferences and workshops such as the MobiWorld, MIST, SeCIHD, and AsiaARES. He is the EiC of the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. He is on the Editorial Board of *Information Sciences*, *Journal of Network and Computer Applications*, *International Journal of Ad Hoc and Ubiquitous Computing*, *Computing and Informatics*, *Journal of High Speed Networks*, *Intelligent Automation and Soft Computing*, and *Security and Communication Networks*.