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]*

***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 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 SH-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 AVISPA. Further, 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 SH-IoT network implementation include surveillance using cameras, leak detections, air concentration check, and temperature control, etc.

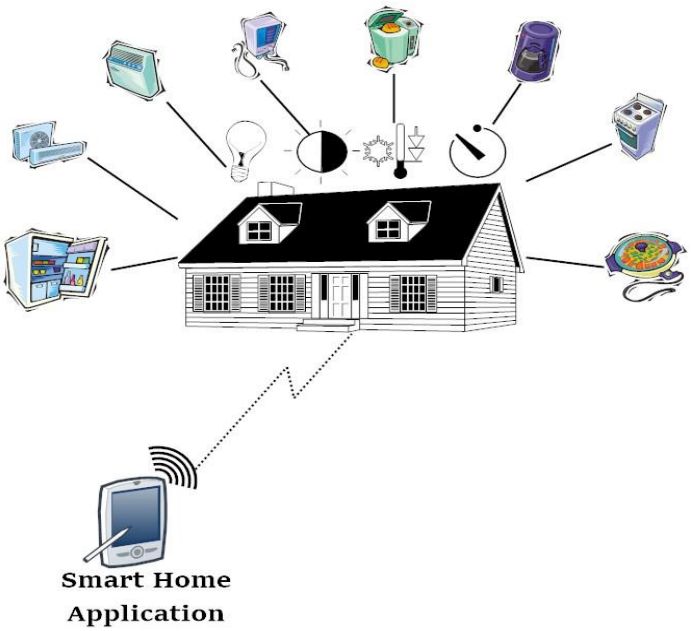

Fig. 1 An illustration of a smart home equipped with various IoT devices.

[1]The authors are with the Department of Information Security Engineering, Soonchunhyang University, Asan-si 31538, The Republic of Korea.
[2]The author is with Financial Security Institute, Republic of Korea.
Corresponding author: Ilsun You, ilsunu@gmail.com..

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2710379, IEEE Access

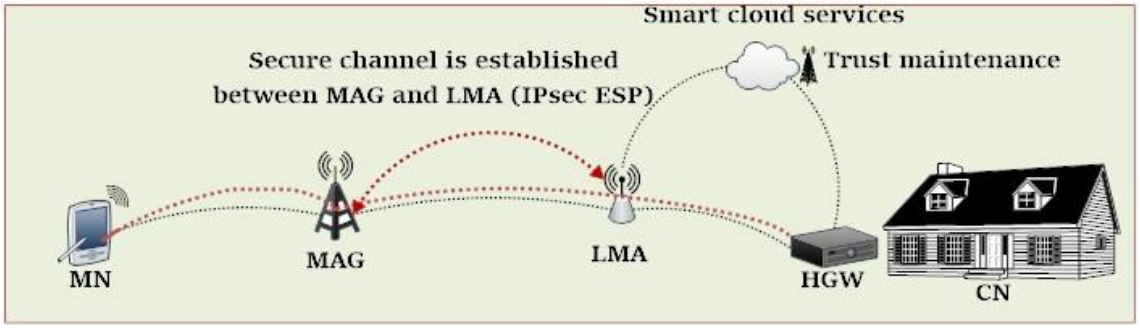

Fig. 2 An illustration of transmission between a mobile node (MN) and corresponding node (CN) via home gateway (HGW), mobile access gateway (MAG), and local mobility anchor (LMA) using PMIPv6. The trust between LMA and HGW is maintained by using the smart cloud services from the network providers.

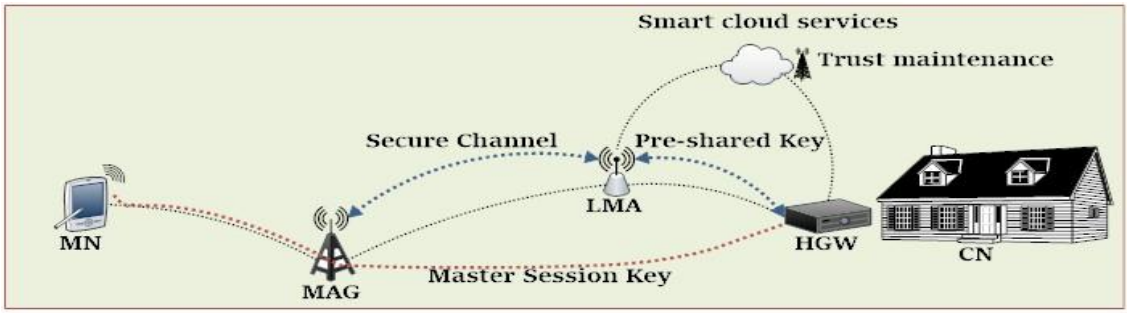

Fig. 3 An illustration of transmission between a mobile node (MN) and corresponding node (CN) using RO strategy over PMIPv6. Note that the 4 session keys are established between MAG and HGW

- SK_i (or SK_i): This key is derived from KLMA-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.

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.

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 from 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, motivation and problem statement

The SH-IoT network communicates with the smart home applications via two intermediate entities, namely, Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA) as stated in Proxy Mobile IPv6 (PMIPv6) [61]. The smart home devices are connected to a Home Gateway (HGW), which serves as the network manager for all the intelligent equipments in a house. The illustrations of problem scenario for SH-IoT network and its solution proposed in this paper are shown in Figs. 2 and 3, respectively. It is assumed that the trust between the HGW and the LMA is maintained by the smart cloud service provider, which makes a log for every address assigned to an HGW. Every HGW user can register itself to the smart cloud service provider before setting up the automation system. In the initial phase, the security is provided by the LMA which interacts with a Mobile Node (MN) via its MAG and with the Corresponding Node (CN) via its HGW. All the IoT devices in the smart home automation system are referred as the CN. Initially, every data is anchored through the LMA which handles the security between the two entities, MAG and HGW.

Every message which is to be transferred to the CN follows a non-optimal path among the MAG, the LMA, and the HGW leading to excessive performance overheads. This excessive transmission phase raises the requirement of RO over the similar or enhanced level of security. Thus, elimination of the excessive dependency over the LMA for every transmission, even after the authentication, is the motivation behind the requirement of a new solution for secure RO in smart home applications.

Every connection between the MN and the CN operates through three entities, MAG, LMA, and HGW. The CN interacts with the HGW since it is the trust builder with the smart cloud service provider, and the MN interacts with the MAG as it controls the mobility and acts as a gateway to the smart home network. The LMA provides channel security to both MAG and HGW. However, the secure channel needs to be established only after the initiation of transmission. Passage of data via the LMA after authentication results in significant performance overheads in the entire network. When a handover decision is made, repetition of the entire procedure through the path MAG–HGW-LMA increases the handover latency, which affects the performance of the entire network. Thus, the problem deals with the elimination of the excessive overheads caused by such a triangular routing that can be resolved by providing secure RO.

B. Our contribution and highlights

In this paper, the problem of secure RO is considered in 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. In order words, 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 cause many overheads despite the level of security. Madakam and Date [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 and Li [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] and Jacobsson and Davidsson [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.

Al 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 and Shen [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 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 research 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

TABLE I
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 authenticatio n	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

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 and Chung [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] [41] [42] [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] [48] [49] [50] [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

MN, *MAG*, *LMA*,	mobile node, mobile access gateway, local mobility anchor,
HGW, *CN*	home gateway, and corresponding node
pMAG and *nMAG*	current and next *MAG*s
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 *i*th session key between *HGW* and the *i*th *MAG*
||	concatenation operation

Fig. 3. Notations and symbols for the proposed approach.

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 I.

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.3.

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 his HGW with the service provider. As a result of this trust relationship, the secret key $K_{LMA-HGW}$ between the PMIPv6 domain and the HGW is shared, $K_{LMA-HGW}$ is 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]]
- The integrity and confidentiality for protection channel based on IPsec ESP are established between the previous MAG and the new MAG; and it is assumed that the handover and RO context of the MN can be securely transmitted to the next MAG.

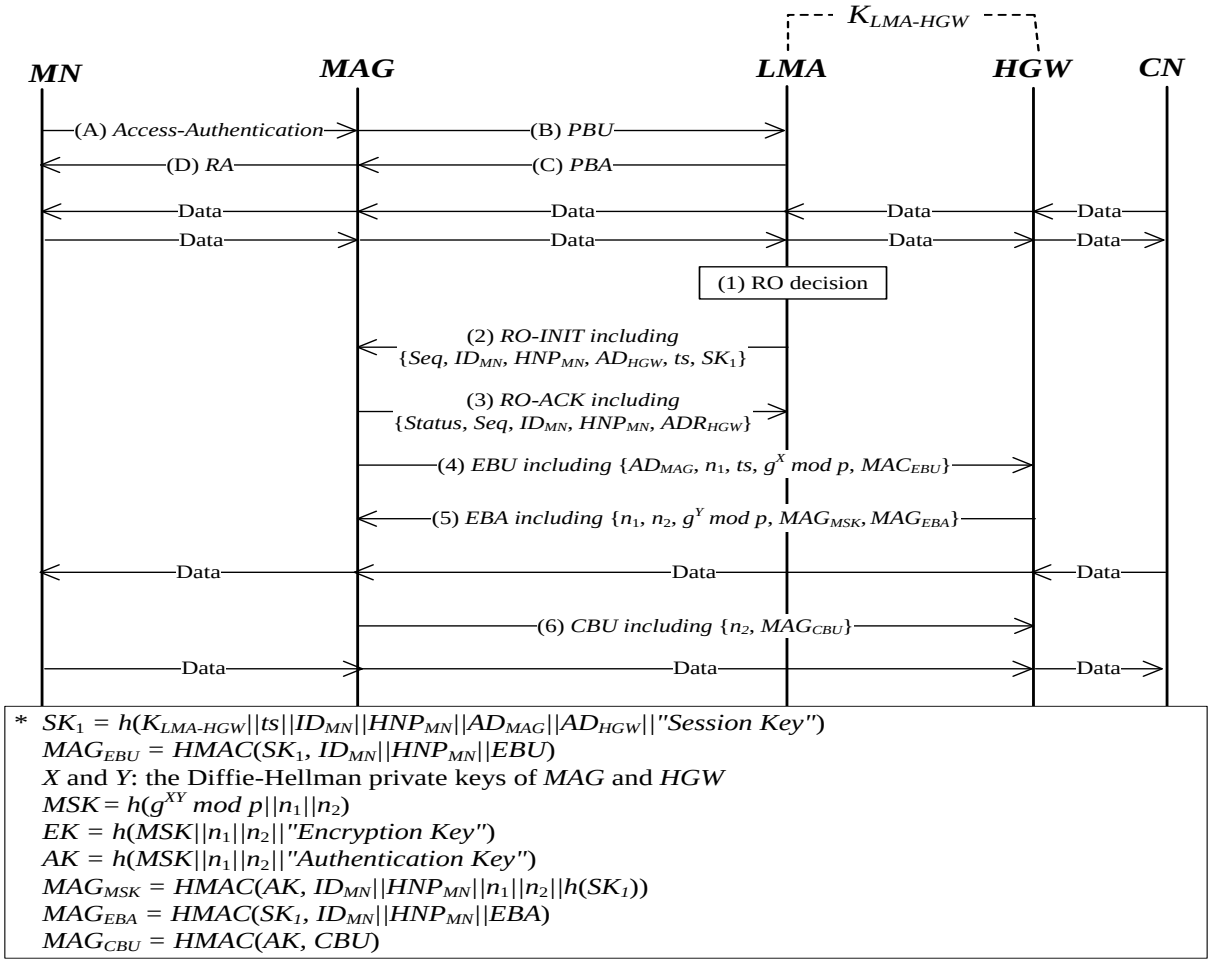

Fig.4 First phase of the proposed approach for RO (RO Initialization Step (RO_INIT Step))

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 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: It is a kind of Denial of Service (DoS) attack. The proposed approach should not be vulnerable to these DoS attacks that lead to 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 and the exchange of the session key with PFS.

A. Route Optimization Initialization Step (RO_INIT)

The RO_INIT process determines whether the route is optimized after initiation of the PMIPv6 Binding Update process, as shown in the Fig. 4. It is activated if the MN has right to perform routing.

In this process, the PMIPv6 entities, MN, MAG and LMA, perform authentication and binding update like existing PMIPv6 before RO decision. When the binding update is

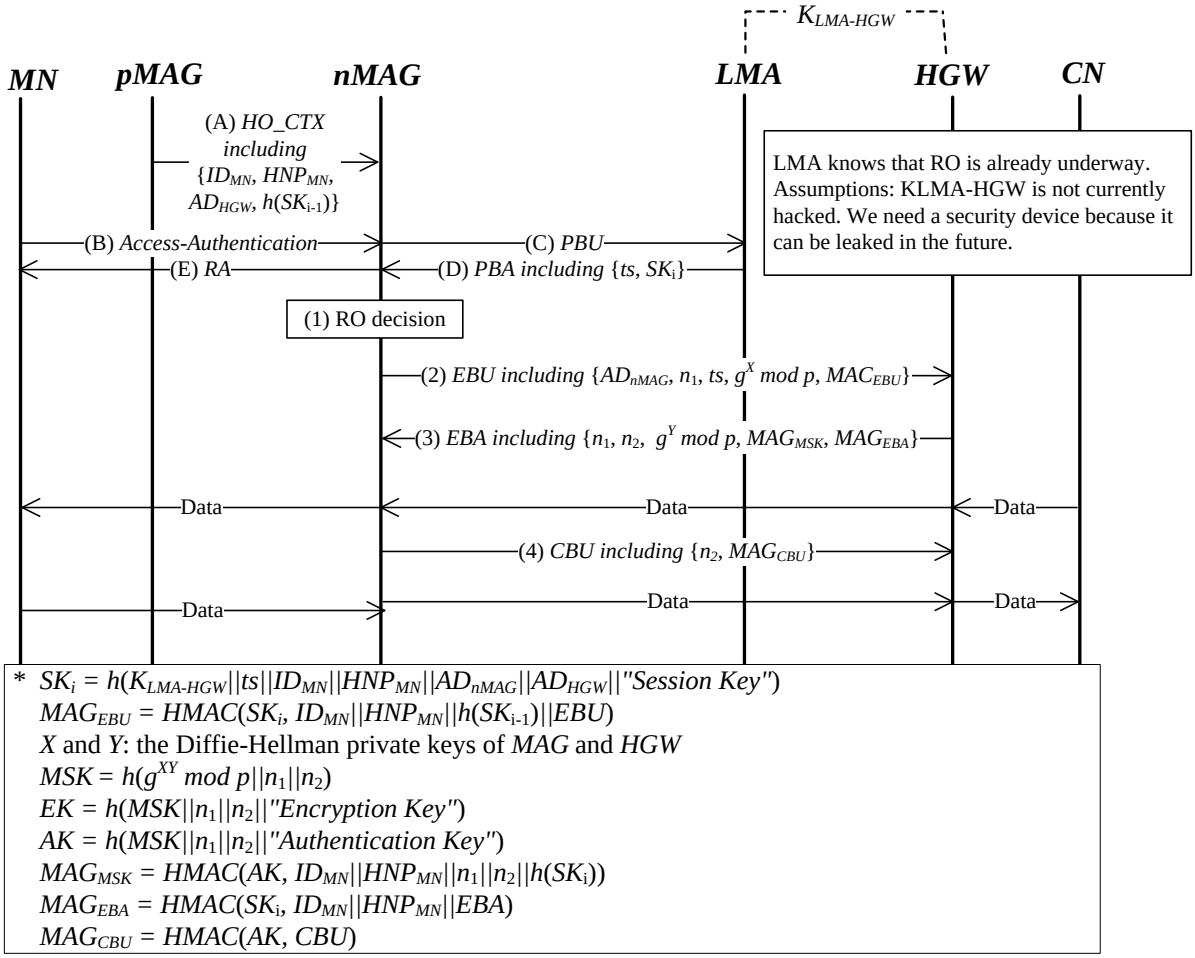

Fig. 5 Second phase of RO (Handover Management Step (RO_HO_MAN Step))

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. 4 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 rights to perform RO, then the traffic is observed to determine whether RO between the two is necessary.[1]

(2)- (3) At first, the LMA exchanges the PR-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 $g^X modp$ 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. The, it generates its own Diffie-Hellman private key Y and public key by $g^Y modp$ 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 such case, the HGW computes $g^{XY} modp$ using the public key $g^X modp$ of the MAG and its own private key, and generates $MSK = h(g^{XY} modp\|n_1\|n_2)$ 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.

[1]Details of the route optimization method are beyond the scope of this paper and are not mentioned here

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

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 $g^Y modp$ 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.5 are explained below:

(1) Before handover from the pMAG to the nMAG by the MN, the pMAG transmits an HO_CTX message including the 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][65][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 of these two tools provides more thoroughly and stronger verification while allowing them to complement each other.

TABLE II
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 Xin 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.

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 II, and the BAN-logic's rules are given below:

Message Meaning Rule (MM)

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

Nonce Verification Rune (NV)

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

Freshness Rule (FR)

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

Belief Conjunction Rule (BC)

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

Diffie-Hellman Rule (DH)

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

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.

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2710379, IEEE Access

$$\text{(I1)} nMAG \rightarrow HGW: \langle \begin{matrix} ID_{MN}, HNP_{MN}, h(SK_{i-1}), \\ AD_{nMAG}, n_1, ts, \xrightarrow{g^X \bmod p} nMAG \end{matrix} \rangle_{SK_i}$$

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

$$where\ MAG_{MSK} = \langle \begin{matrix} ID_{MN}, HNP_{MN}, n_1, n_2, h(SK_i), \\ nMAG \overset{EK}{\leftrightarrow} HGW, nMAG \overset{AK}{\Leftrightarrow} HGW \end{matrix} \rangle_{AK}$$

$$\text{(I3)}\ nMAG \rightarrow HGW: \langle \begin{matrix} n_2, nMAG \overset{EK}{\leftrightarrow} HGW, \\ nMAG \overset{AK}{\Leftrightarrow} HGW \end{matrix} \rangle_{AK}$$

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

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

(A1) $HGW believes nMAG \overset{SK_i}{\Leftrightarrow} HGW$
(A2) $HGW believes \#(ts)$
(A3) $HGW believes \xrightarrow{g^Y \bmod p} HGW$
(A4) $HGW believes \#(n_2)$
(A5) $nMAG believes nMAG \overset{SK_i}{\Leftrightarrow} HGW$
(A6) $nMAG believes \#(n_1)$
(A7) $nMAG believes \xrightarrow{g^X \bmod p} nMAG$

Goals: The goals of our proposed protocol are defined as shown below. The goals (G1) ~ (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) $HGW believes\ nMAG \overset{MSK}{\longleftrightarrow} HGW$
(G5) $HGW believes\ nMAG \overset{AK}{\Leftrightarrow} HGW$
(G6) $HGW believes\ nMAG \overset{EK}{\leftrightarrow} HGW$
(G7) $nMAG\ believes\ nMAG \overset{MSK}{\longleftrightarrow} HGW$
(G8) $nMAG\ believes\ nMAG \overset{AK}{\Leftrightarrow} HGW$
(G9) $nMAG\ believes\ nMAG \overset{EK}{\leftrightarrow} HGW$
(G10) $nMAG\ believes\ HGW\ believes\ nMAG \overset{AK}{\Leftrightarrow} HGW$
(G11) $nMAG\ believes\ HGW\ believes\ nMAG \overset{EK}{\leftrightarrow} HGW$
(G12) $HGW\ believes\ nMAG\ believes\ nMAG \overset{AK}{\Leftrightarrow} HGW$
(G13) $HGW\ believes\ nMAG\ believes\ nMAG \overset{EK}{\leftrightarrow} HGW$

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

From (I1), we derive:

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

$$HGW believes\ nMAG\ believes \begin{pmatrix} ID_{MN}, HNP_{MN}, \\ h(SK_{i-1}), \\ AD_{nMAG}, \\ n_1, ts, \\ \xrightarrow{g^X \bmod p} nMAG \end{pmatrix} \quad (2)$$

$$by\ (1), (A1), \text{MM}, (A2), \text{FR}, \text{NV}$$

$$HGW believes\ nMAG\ believes \begin{pmatrix} ID_{MN}, HNP_{MN}, \\ AD_{nMAG}, h(SK_{i-1}) \end{pmatrix} \quad (3)$$

$$by\ (2), \text{BC}$$

$$HGW believes\ nMAG\ believes \xrightarrow{g^X \bmod p} nMAG \quad (4)$$

$$by\ (2), \text{BC}$$

$$HGW believes\ \ nMAG \xrightarrow{g^{XY} \bmod p} HGW \quad (5)$$

$$by\ (4), (A3), \text{DH}$$

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

$$HGW believes\ \ nMAG \overset{MSK}{\longleftrightarrow} HGW \quad (7)$$
$$by\ (2), BC, (6), (A4), (5)$$

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

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

From (I2), we derive:

$$nMAG sees \langle \begin{matrix} ID_{MN}, HNP_{MN}, n_1, n_2, \xrightarrow{g^Y \bmod p} HGW, \\ nMAG \overset{MSK}{\longleftrightarrow} HGW, MAG_{MSK} \end{matrix} \rangle_{SK_i} \quad (10)$$

$$nMAG\ believes\ HGW\ believes$$

$$\begin{pmatrix} ID_{MN}, HNP_{MN}, n_1, n_2, \xrightarrow{g^Y \bmod p} HGW, \\ nMAG \overset{MSK}{\longleftrightarrow} HGW, MAG_{MSK} \end{pmatrix} \quad (11)$$

$$by\ (10), (A5), \text{MM}, (A6), \text{FR}, \text{NV}$$

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

$$nMAG\ believes\ HGW\ believes \xrightarrow{g^Y \bmod p} HGW \quad (13)$$

$$by\ (11), \text{BC}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2710379, IEEE Access

$$nMAG\ believes\ nMAG \xleftrightarrow{g^{XY}\ mod\ p} HGW \quad by\ (13), (A7), \text{DH} \tag{14}$$

$$nMAG\ believes\ HGW\ believes\ n_2\ by\ (11), \text{BC} \tag{15}$$

$$nMAG\ believes\ nMAG \xleftrightarrow{MSK} HGW \quad by\ (15), (A6), (14) \tag{16}$$

$$nMAG\ believes\ nMAG \overset{AK}{\Leftrightarrow} HGW\ by\ (16) \tag{17}$$

$$nMAG\ believes\ nMAG \overset{EK}{\leftrightarrow} HGW\ by\ (16) \tag{18}$$

$$nMAG\ sees \left\langle \begin{matrix} ID_{MN}, HNP_{MN}, n_1, n_2, h(SK_i), \\ nMAG \overset{EK}{\leftrightarrow} HGW, nMAG \overset{AK}{\Leftrightarrow} HGW \end{matrix} \right\rangle_{AK} \quad by\ (11), \text{BC} \tag{19}$$

$$nMAG\ believes\ HGW\ believes \left(\begin{matrix} ID_{MN}, HNP_{MN}, n_1, \\ n_2, h(SK_i), nMAG \overset{EK}{\leftrightarrow} HGW, nMAG \overset{AK}{\Leftrightarrow} HGW \end{matrix} \right) \quad by\ (19), (17), \text{MM}, (A6), \text{FR}, \text{NV} \tag{20}$$

$$nMAG\ believes\ HGW\ believes\ nMAG \overset{EK}{\leftrightarrow} HGW \quad by\ (20), \text{BC} \tag{21}$$

$$nMAG\ believes\ HGW\ believes\ nMAG \overset{AK}{\Leftrightarrow} HGW \quad by\ (20), \text{BC} \tag{22}$$

From (I3), we derive:

$$HGW sees \langle n_2, nMAG \overset{EK}{\leftrightarrow} HGW, nMAG \overset{AK}{\Leftrightarrow} HGW \rangle_{AK} \tag{23}$$

$$HGW believes\ nMAG\ believes \left(n_2, nMAG \overset{EK}{\leftrightarrow} HGW, nMAG \overset{AK}{\Leftrightarrow} HGW \right) \quad by\ (23), (8), \text{MM}, (A4), \text{FR}, \text{NV} \tag{24}$$

$$HGW believes\ nMAG\ believes\ nMAG \overset{EK}{\leftrightarrow} HGW \quad by\ (24), \text{BC} \tag{25}$$

$$HGW believes\ \ nMAG\ believes\ nMAG \overset{AK}{\Leftrightarrow} HGW \quad by\ (24), \text{BC} \tag{26}$$

$$HGW believes\ n_2\ \text{by}\ (24), \text{BC} \tag{27}$$

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) ~ (G9) are satisfied with the beliefs (7) ~ (9) and (16) ~ (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 authenticates 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):

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

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, $K_{LMA\text{-}HGW}$, 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

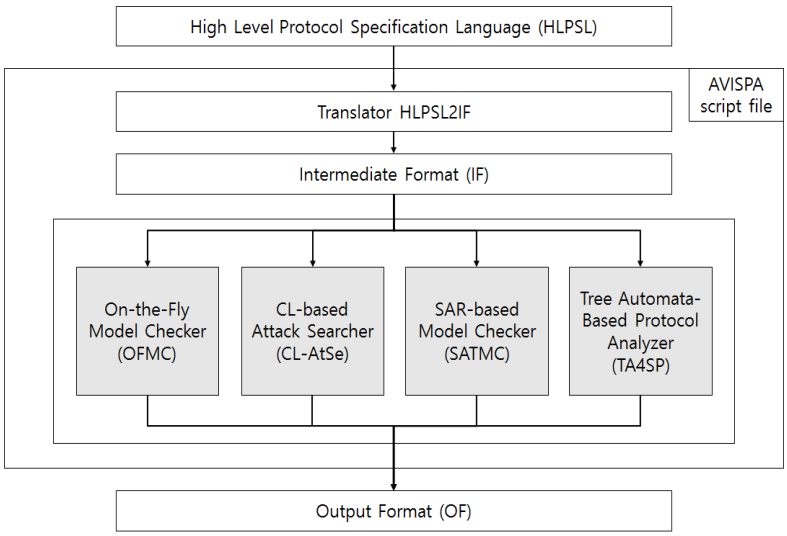

Fig. 6 Architecture of AVISPA

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}, 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 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 create 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.6 presents the operational architecture of AVISPA.The proposed RO protocol is divided into the previous session and the future session on the basis of handovers.

A separate RO protocol is proposed for each session, and protocols for each session are analyzed and verified through AVISPA. Before examining the results of the proposed RO protocol, we briefly describe the specification of each protocol. The route optimization protocol, prior to handover consists of four roles, namely, as MN, MAG, LMA, and HGW. After the handover, the RO protocol consists of 5 roles, which are specified as MN, pMAG (previous MAG), nMAG (new MAG), LMA and HGW as shown in Fig. 7 and Fig. 8. The results obtained from the analysis using AVISPA suggest that the protocol is safe and accounts with the BAN-logic and can be readily applied to smart home IoT networks. The detailed results are given in Appendix-I.

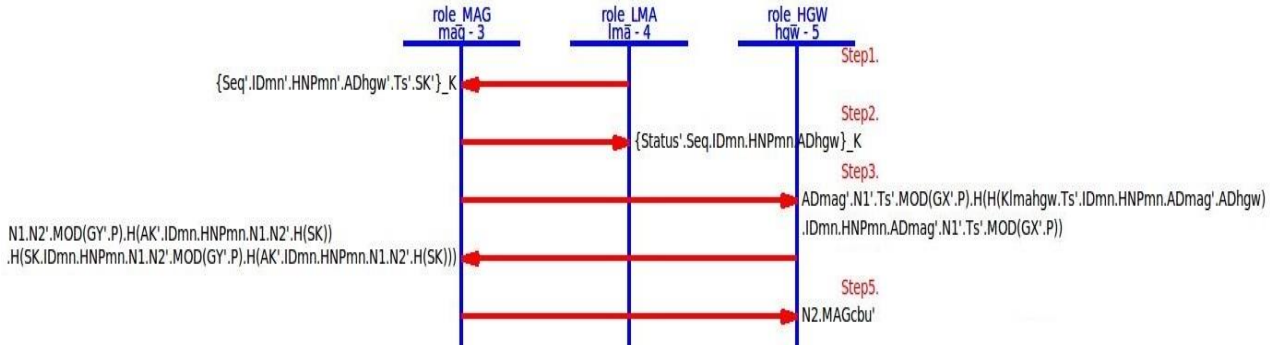

Fig.7 Flow of RO-INIT step

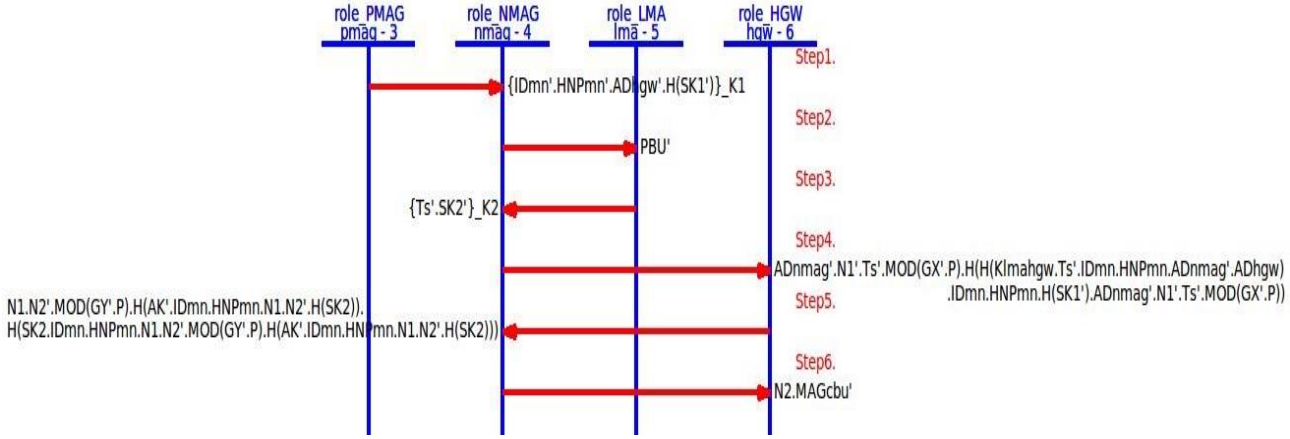

Fig.8 Flow of RO-HO-MAN step

Table III.
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

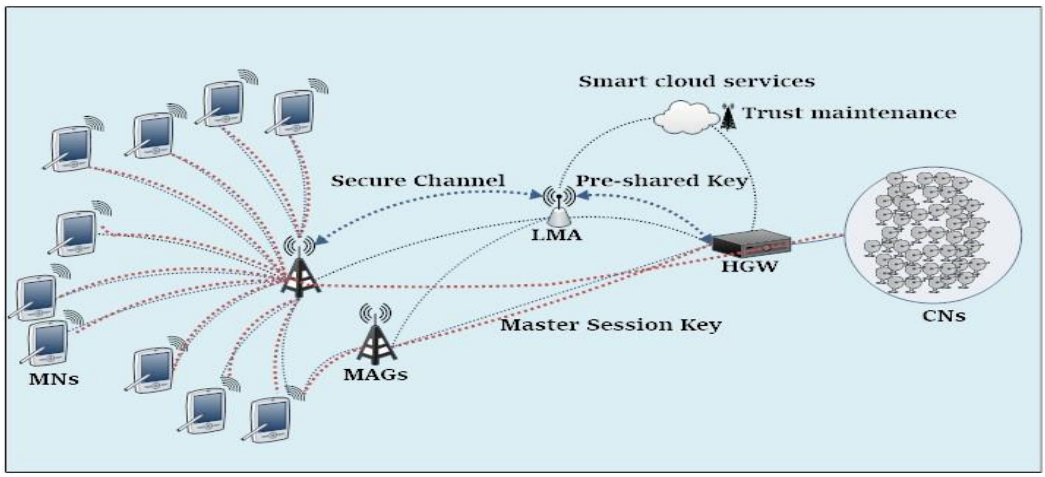

Fig. 9 An illustration of the simulation scenario considered for evaluation of the proposed approach.

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. Each 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 III with a simulation scenario in Fig 9.

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.10. 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.

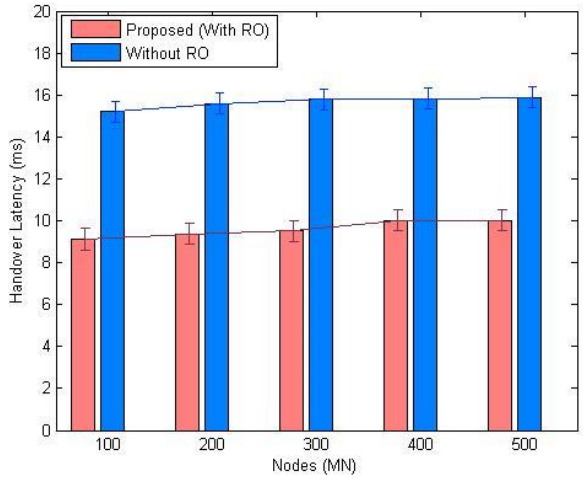

Fig. 10 Handover latency vs. nodes.

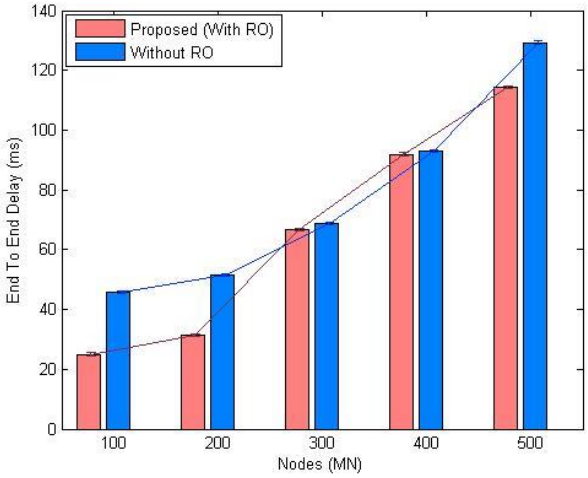

Fig. 11 End to End Delay vs. nodes.

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.11. 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.12 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.

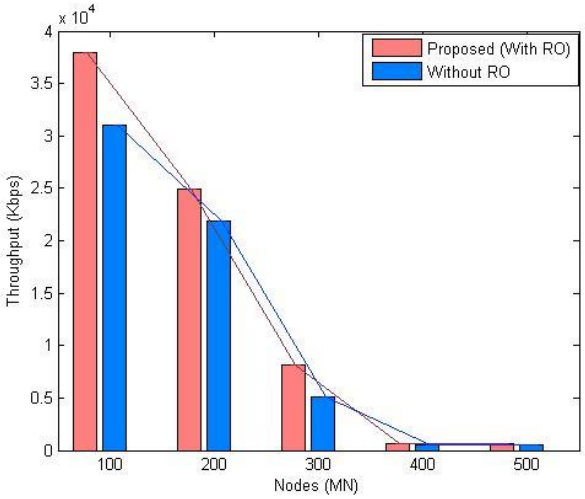

Fig. 12 Network Throughput vs. nodes.

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.

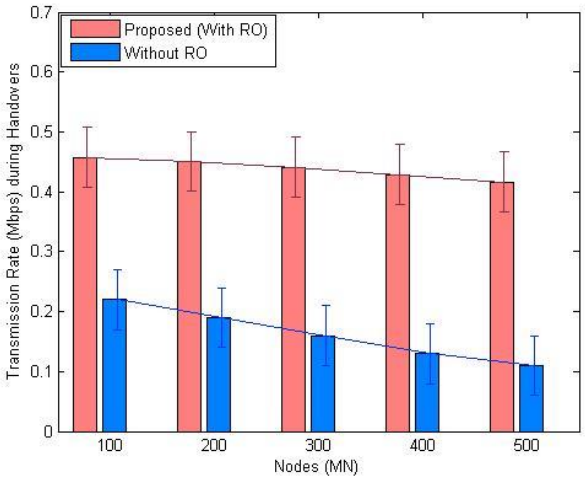

Fig. 13 Transmission rate during handovers vs. nodes.

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.13. 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.

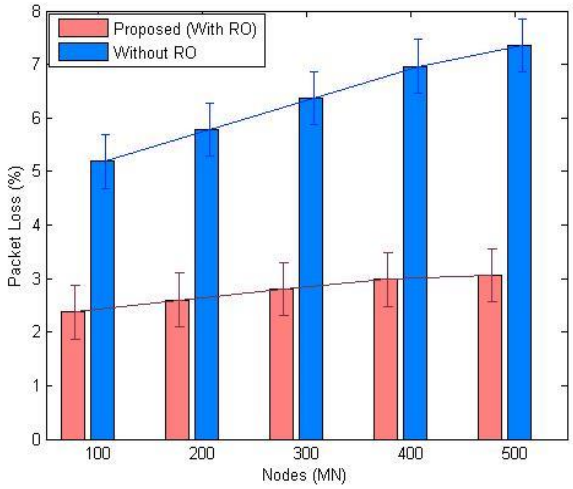

Fig. 14 Packet loss vs. nodes.

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, the proposed approach provides higher delivery support and less packet loss as shown in Fig.14.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, and performance will be evaluated using varying traffic and mobility models.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2016R1D1A1B03935619) as well as by the Soonchunhyang University Research Fund.

APPENDIX-I

In this appendix, the proposed protocol is specified using HLPSL and verified with OFMC and CL-AtSe among the sub-modules of AVISPA. Figs. 15 and 16 show the results of verification of proposed RO protocol before handover with OFMC and CL-AtSe. Fig. 17 and Fig. 18 show the result of verification for the path of proposed RO protocol after handover with OFMC and CL-AtSe, respectively. These results correspond to the theoretical analysis, and prove that the proposed RO protocol is safe to attacks.

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/asdf.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.04s
 visitedNodes: 12 nodes
 depth: 6 plies
```

Fig.15 The output of OFMC back-end (RO-INIT step)

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

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

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed  : 8 states
 Reachable  : 6 states
 Translation: 0.05 seconds
 Computation: 0.00 seconds
```

Fig.16 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/IoT_2.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.02s
 visitedNodes: 7 nodes
 depth: 4 plies
```

Fig.17 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/IoT_2.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed  : 8 states
 Reachable  : 3 states
 Translation: 0.04 seconds
 Computation: 0.00 seconds
```

Fig.18 The output of CL-AtSe back-end (RO-HO-MAN step)

REFERENCES

[1] Jose, Arun Cyril, Reza Malekian, and Ning Ye. "Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home." IEEE Access 4 (2016): 5776-5787.

[2] Kennedy, Zachery Webster, Ted Boda, Jeffrey Alan Boyd, Jeffery Theodore Lee, Jesse Boettcher, David Hendler Sloo, Michael Mizono, Tomas Brennessl, James Simister, and Anton Davydov. "Home security system with automatic context-sensitive transition to different modes." U.S. Patent 9,501,924, issued November 22, 2016.

[3] Islam, Kamrul, Weiming Shen, and Xianbin Wang. "Security and privacy considerations for wireless sensor networks in smart home environments." In Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on, pp. 626-633. IEEE, 2012.

[4] Kumar, Pardeep, Andrei Gurtov, Jari Iinatti, Mika Ylianttila, and Mangal Sain. "Lightweight and secure session-key establishment scheme in smart home environments." IEEE Sensors Journal 16, no. 1 (2016): 254-264.

[5] Peter, Sherin, and Raju K. Gopal. "Multi-level authentication system for smart home-security analysis and implementation." In Inventive Computation Technologies (ICICT), International Conference on, vol. 2, pp. 1-7. IEEE, 2016.

[6] Stout, William MS, and Vincent E. Urias. "Challenges to securing the Internet of Things." In *Security Technology (ICCST), 2016 IEEE International Carnahan Conference on*, pp. 1-8. IEEE, 2016.

[7] Robles, Rosslin John, Tai-hoon Kim, D. Cook, and S. Das. "A review on security in smart home development." International Journal of Advanced Science and Technology, 15 (2010), pp.13-22.

[8] Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." In *Security and Privacy (SP), 2016 IEEE Symposium on*, pp. 636-654. IEEE, 2016.

[9] Wang, Yan, Yanqing Zhao, Shuming Jiang, Haizhou Feng, Fengjiao Li, and Juechen Wang. "Design of the Smart-home Security System based on Cloud Computing." DEStech Transactions on Engineering and Technology Research iect (2016), doi: 10.12783/dtetr/iect2016/3714

[10] Madakam, Somayya, and Hema Date. "Security Mechanisms for Connectivity of Smart Devices in the Internet of Things." In *Connectivity Frameworks for Smart Devices*, pp. 23-41. Springer International Publishing, 2016.

[11] Brauchli, Andreas, and Depeng Li. "A solution based analysis of attack vectors on smart home systems." In *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*, pp. 1-6. IEEE, 2015.

[12] Jacobsson, Andreas, Martin Boldt, and Bengt Carlsson. "A risk analysis of a smart home automation system." *Future Generation Computer Systems* 56 (2016): 719-733.

[13] Jacobsson, Andreas, and Paul Davidsson. "Towards a model of privacy and security for smart homes." In *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*, pp. 727-732. IEEE, 2015.

[14] Ge, Mengmeng, Jin B. Hong, Walter Guttmann, and Dong Seong Kim. "A framework for automating security analysis of the internet of things." *Journal of Network and Computer Applications* 83 (2017): 12-27.

[15] Nobakht, Mehdi, Vijay Sivaraman, and Roksana Boreli. "A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow." In *Availability, Reliability and Security (ARES), 2016 11th International Conference on*, pp. 147-156. IEEE, 2016.

[16] Fernandes, Francisco Erivaldo, Guanci Yang, Ha Manh Do, and Weihua Sheng. "Detection of privacy-sensitive situations for social robots in smart homes." In *Automation Science and Engineering (CASE), 2016 IEEE International Conference on*, pp. 727-732. IEEE, 2016.

[17] Perkins, Charles E. "Securing Mobile IPv6 route optimization using a static shared key." (2006), IETF RFC 4449

[18] Johnson, David, Charles Perkins, and Jari Arkko. *Mobility support in IPv6*. No. RFC 3775. 2004..

[19] Barbudhe, Aumdevi K., Vishwajit K. Barbudhe, and Chitra Dhawale. "Comparative analysis of security mechanism of mobile IPv6 threats against binding update, Route Optimization and Tunneling." In *Adaptive Science & Technology (ICAST), 2014 IEEE 6th International Conference on*, pp. 1-7. IEEE, 2014.

[20] Ren, Kui, Wenjing Lou, Kai Zeng, Feng Bao, Jianying Zhou, and Robert H. Deng. "Routing optimization security in mobile IPv6." *Computer Networks* 50, no. 13 (2006): 2401-2419.

[21] Kavitha, Dwaram, KE Sreenivasa Murthy, and S. Zahoor ul Huq. "Security analysis of binding update protocols in route optimization of MIPv6." In *Recent Trends in Information, Telecommunication and Computing (ITC), 2010 International Conference on*, pp. 44-49. IEEE, 2010.

[22] Song, Sehwa, Hyoung-Kee Choi, and Jung-Yoon Kim. "A secure and lightweight approach for routing optimization in mobile IPv6." *EURASIP Journal on Wireless Communications and Networking* 2009, no. 1 (2009): 957690.

[23] Al Hawi, Faisal, Chan Yeob Yeun, and Khaled Salah. "Secure framework for the return routability procedure in MIPv6." In *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, pp. 1386-1391. IEEE, 2013.

[24] Mehdizadeh, Abbas, Sabira Khatun, Borhanuddin Mohd Ali, RSA Raja Abdullah, and G. Kurup. "Secured route optimization in mobile IPv6 wireless networks in terms of data integrity." In *Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on*, pp. 643-646. IEEE, 2008.

[25] Mehdizadeh, Abbas, Sabira Khatun, Borhanuddin M. Ali, RSA Raja Abdullah, and Gopakumar Kurup. "Route Optimization Security in Mobile IPv6 Wireless Networks: A Test-Bed Experience." In *Advances in Computer Science and Engineering*, pp. 153-159. Springer Berlin Heidelberg, 2008.

[26] Rossi, Angelo, Samuel Pierre, and Suresh Krishnan. "Secure route optimization for MIPv6 using enhanced CGA and DNSSEC." *IEEE Systems Journal* 7, no. 3 (2013): 351-362.

[27] Diana, A. Avelin, V. Ragavinodhini, K. Sundarakantham, and S. Mercy Shalinie. "SHAD: Swift Home Agent Discovery mechanism to mitigate home registration latency in MIPv6 Network." *International Information Institute (Tokyo). Information* 17, no. 4 (2014): 1375.

[28] Taha, Sanaa, and Xuemin Sherman Shen. "ALPP: anonymous and location privacy preserving scheme for mobile IPv6 heterogeneous networks." *Security and Communication Networks* 6, no. 4 (2013): 401-419.

[29] You, Ilsun. "A ticket based binding update authentication method for trusted nodes in mobile IPv6 domain." In International Conference on Embedded and Ubiquitous Computing, pp. 808-819. Springer Berlin Heidelberg, 2007.

[30] You, Ilsun, Jong□Hyouk Lee, and Bonam Kim. "caTBUA: Context□ aware ticket□based binding update authentication protocol for trust□ enabled mobile networks." *International Journal of Communication Systems* 23, no. 11 (2010): 1382-1404.

[31] Lee, Jae-Min, Jong-Hyouk Lee, and Tai-Myoung Chung. "Performance analysis of route optimization on proxy mobile IPv6." In *Systems and Networks Communications, 2008. ICSNC'08. 3rd International Conference on*, pp. 280-285. IEEE, 2008.

[32] Guan, Jianfeng, Ilsun You, Changqiao Xu, Huachun Zhou, and Hongke Zhang. "Survey on route optimization schemes for proxy mobile IPv6." In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, pp. 541-546. IEEE, 2012.

[33] Raza, Syed M., Pankaj Thorat, Rajesh Challa, Hyunseung Choo, and Dongsoo S. Kim. "SDN based inter-domain mobility for PMIPv6 with route optimization." In *NetSoft Conference and Workshops (NetSoft), 2016 IEEE*, pp. 24-27. IEEE, 2016.

[34] Kim, P., S. Kim, J. Jin, and S. Lee. "Proactive correspondent registration for Proxy Mobile IPv6 route optimization." *IJCSNS International Journal of Computer Science and Network Security* 7, no. 11 (2007): 149-155.

[35] Leu, Fang-Yie, Chin-Yu Liu, Jung-Chun Liu, Fuu-Cheng Jiang, and Heru Susanto. "S-PMIPv6: An intra-LMA model for IPv6 mobility." *Journal of Network and Computer Applications* 58 (2015): 180-191.

[36] Han, Byung-Jin, Jae-Min Lee, Jong-Hyouk Lee, and Tai-Myoung Chung. "PMIPv6 route optimization mechanism using the routing table of MAG." In *Systems and Networks Communications, 2008. ICSNC'08. 3rd International Conference on*, pp. 274-279. IEEE, 2008.

[37] Chiba, Tsunehiko, Hidetoshi Yokota, Ashutosh Dutta, Dana Chee, and Henning Schulzrinne. "Route optimization for proxy mobile IPv6 in IMS network." In *Signal Processing and Communication Systems, 2008. ICSPCS 2008. 2nd International Conference on*, pp. 1-9. IEEE, 2008.

[38] Choi, Young-Hyun, and Tai-Myoung Chung. "Using Correspondent Information for Route Optimization Scheme on Proxy Mobile IPv6." *JNW* 5, no. 8 (2010): 984-989.

[39] Kang, Byungseok, Namyeong Kwon, and Hyunseung Choo. "Developing route optimization-based PMIPv6 testbed for reliable packet transmission." *IEEE Access* 4 (2016): 1039-1049.

[40] Wang, Yumei, Yufei Feng, and Lin Zhang. "Coordinating fast handover and route optimization in proxy mobile IPv6." In *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*, pp. 1-4. IEEE, 2009.

[41] Chuang, Ming-Chin, Jeng-Farn Lee, and Meng-Chang Chen. "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks." *IEEE Systems Journal* 7, no. 1 (2013): 102-113.

[42] Hwang, Seok Hyun, Jin Ho Kim, Choong Seon Hong, and Jung-Sik Sung. "Localized management for proxy mobile IPv6." In *Int Conf on Information Networking, ICOIN*. 2010.

[43] Sihun, P. A. R. K., K. A. N. G. Namhi, and K. I. M. Younghan. "Localized proxy-MIPv6 with route optimization in IP-based networks." *IEICE transactions on communications* 90, no. 12 (2007): 3682-3686.

[44] Rasem, Ahmad, Marc St-Hilaire, and Christian Makaya. "Efficient handover with optimized localized routing for Proxy Mobile IPv6." *Telecommunication Systems* 62, no. 4 (2016): 675-693.

[45] Rasem, Ahmad, Christian Makaya, and Marc St-Hilaire. "O-PMIPv6: Efficient handover with route optimization in proxy mobile IPv6 domain." In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*, pp. 47-54. IEEE, 2012.

[46] Cho, Chulhee, Jae-Young Choi, Jongpil Jeong, and Tai-Myoung Chung. "Performance Analysis of Inter-Domain Handoff Scheme Based on Virtual Layer in PMIPv6 Networks for IP-Based Internet of Things." *PloS one* 12, no. 1 (2017): e0170566.

[47] Guan, Jianfeng, Huachun Zhou, Zhiwei Yan, Yajuan Qin, and Hongke Zhang. "Implementation and analysis of proxy MIPv6." *Wireless Communications and Mobile Computing* 11, no. 4 (2011): 477-490.

[48] Jabir, Adnan J., S. Shamala, Z. Zuriati, and Nawa Hamid. "A comprehensive survey of the current trends and extensions for the proxy mobile IPv6 protocol." *IEEE Systems Journal* (2015).

[49] Modares, Hero, Amirhosein Moravejosharieh, Jaime Lloret, and Rosli Bin Salleh. "A survey on proxy mobile IPv6 handover." *IEEE Systems Journal* 10, no. 1 (2016): 208-217.

[50] Won-Kyeong, S. E. O., 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 transactions on communications* 95, no. 10 (2012): 3149-3157.

[51] Kong, Ki-Sik. "A PMIPv6-Based Auxiliary Mobility Management Considering Traffic Locality." In *International Conference on Computer Science and its Applications*, pp. 1053-1058. Springer Singapore, 2016.

[52] Baek, Jaejong. "Secure Pre-authentication Schemes for Fast Handoff in Proxy Mobile IPv6." *Journal of information and communication convergence engineering* 14, no. 2 (2016): 89-96.

[53] Magagula, Linoh A., and H. Anthony Chan. "Early discovery and pre-authentication in proxy MIPv6 for reducing handover delay." In *Broadband Communications, Information Technology & Biomedical Applications, 2008 Third International Conference on*, pp. 280-285. IEEE, 2008.

[54] Tripathi, Arun Kumar, R. Radhakrishnan, and J. S. Lather. "Optimized and Secure Authentication Proxy Mobile IPv6 (OS-PMIPv6) Scheme for reducing packet loss." *International Journal of Computer Science and Information Security* 14, no. 6 (2016): 510.

[55] Gao, Tianhan, Ling Tan, Peiyu Qiao, and Kangbin Yim. "An Access Authentication Scheme Based on Hierarchical IBS for Proxy Mobile IPV6 Network." *Intelligent Automation & Soft Computing* 22, no. 3 (2016): 389-396.

[56] You, Ilsun, Jae Deok Lim, Jeong Nyeo Kim, Hyobeom Ahn, and Chang Choi. "Adaptive authentication scheme for mobile devices in proxy MIPv6 networks." *IET Communications* 10, no. 17 (2016): 2319-2327.

[57] Liebsch, Marco, and Sangjin Jeong. "Proxy mobile IPv6 (PMIPv6) localized routing problem statement." (2011), IETF draft.

[58] Wu, Q., and J. Korhonen. "Problem Statement of IPv4 Support for PMIPv6 Localized Routing." *draft-wu-netext-pmipv6-ipv4-ro-ps-00, IETF draft* (2009).

[59] Krishnan, S., R. Koodli, P. Loureiro, Q. Wu, and A. Dutta. *Localized routing for proxy mobile IPv6*. No. RFC 6705. 2012.

[60] Kent, S. "IP Encapsulating Security Payload (ESP)", https://www.ietf.org/rfc/rfc4303.txt, IETF RFC-4303

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

[62] (https://en.wikipedia.org/wiki/Resource_exhaustion_attack) [Last accessed on March 8, 2017]

[63] Burrows, Michael, Martin Abadi, and Roger M. Needham. "A logic of authentication." In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 426, no. 1871, pp. 233-271. The Royal Society, 1989.

[64] You, Ilsun, Yoshiaki Hori, and Kouichi Sakurai. "Enhancing SVO Logic for Mobile IPv6 Security Protocols." *JoWUA* 2, no. 3 (2011): 26-52.

[65] You, Ilsun, Yoshiaki Hori, and Kouichi Sakurai. "Towards formal analysis of wireless LAN security with MIS protocol." *International Journal of Ad Hoc and Ubiquitous Computing* 7, no. 2 (2011): 112-120.

[66] You, Ilsun, and Fang-Yie Leu. "Comments on "SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks"." *IEEE Systems Journal* (2015).https://doi.org/10.1109/JSYST.2015.2477415

[67] Issariyakul, Teerawat, and Ekram Hossain. Introduction to network simulator NS2. Springer Science & Business Media, 2011.

[68] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone, (1997). Handbook of Applied Cryptography. CRC Pres. ISBN 0-8493-8523-7.

[69] Viganò, Luca. "Automated security protocol analysis with the AVISPA tool." Electronic Notes in Theoretical Computer Science 155 (2006): 61-86.