A security protocol for route optimization in DMM based smart home IOT Network

Tushar Agarwal

Computer science & engineering

Abstract: The communication in the Smart Home Internet of Things (SH-IoT) comprising various electronic devices and sensors is very sensitive and crucial. It is also expected that in 5G networks, future smart home services will be much powered by mobility management, 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. As a major solution, Distributed IP Mobility Management (DMM) can be considered because it addresses the limitation of the centralized approaches as well as its flat architecture is suit for 5G networks.

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 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 work now 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 row 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,*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 Use of light weight and secure session key approach can also provide security in smart homes Multilevel authentication
can be a strong solution to security and privacy issues in smart home automation systems Distributed
security solutions can also enhance the channel security of smart homes operating with a large number of IoT devices 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 update among the network entities. Further, the existing solutions leverage excessive burden on the network during handovers.

Smart home network

Design and Implementation of Security for Smart Home based on GSM technology was discussed by Govindan et al. (2014) that provides two methods to implement home security using IoT [1]. One is using web cameras such that whenever there is any motion detected by the camera, it sounds an alarm and sends a mail to the owner. This method of detecting intrusion is quite good, albeit somewhat expensive due to the cost of the cameras involved in the process. The cameras need to be of good quality which means it should have a wide range and the picture quality should be high enough to detect movement. Also if you go for movable cameras such as dome cameras they will cost even more than the fixed ones. SMS based system using GSM was proposed by Karri and Daniel (2005) propose to use internet services to send messages or alert to the house owner instead of the conventional SMS.[2] Jayashree and Arvind (2013) have implemented a fingerprint-based authentication system to unlock a door [3]. This system helps users by only allowing the users whose fingerprint are authorized by the owner of the house. This system can also be used to monitor who all have used the sensor to gained entry into the house. The system is coupled with a few more home protection features such as gas leakage and fire accidents. Although a good system, fingerprint sensors are expensive and complex (as they need increased sensor resolution) to integrate into an IoT setup. Some experts also argue that only relying on a fingerprint sensor is not wise as it is relatively easy to lift someone's fingerprints and replicate them, which is why it is always advised to use fingerprint scanners in a two factor authentication systems where an additional layer of security is available in the form of PIN, passcode, voice recognition, etc. Some researchers proposed an idea of robust IoT home security system where a fault in of one component in the system does not lead to the failure of the whole system [4]. The idea of using multiple devices which may or may not be directly compatible with each other but can be made to work in such a way that they can replace an existing component of the system in case of a fault. In tandem to this, the model has the ability to use overlap between various devices which would result in preserving energy thus making the model more efficient. An example provided of the said model would use temperature sensor, WIFI module and a door sensor to replace a faulty camera. The authors are successful in an effort to demonstrate the given example. However, such systems are useful for people with energy efficiency in mind and for those who need a high degree of robustness with their security systems and are willing to expend more money than usual. Laser rays and LDR sensor are used to to detect intrusion using their movement was proposed in 2016 [5]. The way the system works is that a laser is focused towards a LDR sensor and the moment that the contact of laser to LDR sensor breaks, the alarm connected to the sensor goes off alerting the neighbors and sends a SMS to the owner. This system solves the problem of covering the places which are out of range from the fixed cameras but faces the same difficulties which are faced with systems consisting of GSM modules to send text messages, which is that the delivery of message is dependent on network coverage. Also due to the nature of lasers being a straight beam, it can be avoided by intruders who know about the system and are capable of dodging the lasers, rendering

the whole system useless. A novel way to design an electronic lock using Morse code and IoT technology [6]. The authors claim that this as an original idea which have not been tried before and is the first of its kind “optical Morse code-based electronic locking system”. This system uses LED‟s (Light emitting diodes) as an encrypting medium to send signals. To make it more accessible to general public, the LED in smart phones has been used. On the receiver’s side is a photosensitive resistor as well as a microcontroller such as Arduino processor which has the ability to decrypt the optical signal after receiving them from the LED. Upon decoding the signal, it can than upload the current condition of the lock to a cloud from where the owner can monitor the system. The authors have experimented the system in real time and it has proved to work under different illumination environments with all the functions working as they were intended to. The authors also claim to have an easy and user-friendly interface. The IoT system developed here works very well and can be used by anyone and is very convenient due to the use of mobile phones as LED, which also makes it a cost expensive alternative [7]. Anitha et al (2016) proposed an home automation system using artificial intelligence and also proposed a model for cyber security systems [8,9].

Materials:

1. Arduino Uno
   Arduino is an open source, PC paraphernalia and programming organization, endeavor, and client group that plans and produce microcontroller packs for constructing programmed devices and intelligent object that can detect and control questions in the real world. The inception of the Arduino extends began at the Interaction Design Institute in Ivrea, Italy. The equipment reference plans are appropriated under a Creative Commons Attribution Share.

Smart home security

Choosing a home security system can seem overwhelming but it needn't be that way.

You can tailor your surveillance system to suit your budget and requirements with much less hassle than you might imagine.

Perhaps you're looking to build a new system from the ground up?

Maybe you already have a system in place and you need takeover home security so a new company can assume control of that existing system?

Either way, it pays to have a thorough understanding of your myriad options when it comes to the most effective smart home security system.

Before we explore the different elements of effective indoor and outdoor home security, here's a brief overview of the 3 main types of home security you can introduce…

- **Basic Home Security**
- Intermediate Home Security
- Advanced Smart Home Security

Basic Home Security

If you want to keep things really simple, you can get started with something as straightforward as a **single sensor entry alarm**.

With these devices, you pop a magnet onto your door or window with the sensor and tiny alarm unit nearby. When the magnetic field is breached, you'll hear a piercing alarm so with this small step alone, you'll much safer in your home.

Intermediate Home Security

If you want to step things up a notch, **dial-out security systems** make use of an emergency dialer to alert your smart phone, a family member, or your local security company in the event of a trigger.

These more robust alarm kits can be built out with multiple sensors. You can also incorporate flood, smoke, and temperature sensors to widen the scope of your home security.

Installation is super-simple and these units are pretty user-friendly even if you're not the biggest tech-lover. This is a great way to get started into more ambitious home security systems without too much commitment.

Advanced Smart Home Security

With a **smart home security system**, you harness your home WiFi network so you can monitor and also control a range of security devices in-app from your smart phone.

Thanks to the Internet of Things, you can remotely control door locks and lights to streamline your entry and exit using nothing but your phone. Control extends to thermostats, sprinkler systems, and even pet feeders.

Alongside sensors and motion detectors, you'll need a hub to enable communication with your security devices using Z-Wave, Zigbee, WiFi or a mesh network like Instron.

Deeper home security systems include surveillance cameras inside and in the garden, smoke detectors, water detectors and various audible alarms and floodlighting.

So…

We'll get started with a selection of approaches to **security cameras** before moving on to **locks**, **motion sensors** and full **alarm systems**.

1) Security Cameras

Perhaps you're looking at all the elements of a successful home security system and thinking a straight-up security camera would be more than enough for you.

If that's the case, you've got plenty of options covering indoors and outdoors.

Entry-level video doorbell cameras let you see who's at the door without having to get up.

Connected to your home WiFi, you'll be alerted when anyone approaches the door. You can then communicate with them using your smart phone.

The added benefit is that you'll be able to keep your eyes on things afar so you really can relax on vacation confident your home is fully secured.

The vast bulk of doorbell cameras use the wiring in place for your doorbell while other battery-powered units are extremely easy to install.

Ring dominates the home security space with their user-friendly, tech-driven appliances for all aspects of your smart home.

Although the design is sleek and understated, the doorbell itself is pretty bulky at 5 x 2 ½ x 1 inches so think twice if you live somewhere with restricted doorframe space. The advantage you'll get in return for this added bulk is space to accommodate a battery that should last a year.

Wire the Ring to your exisiting bell or use it separately. While set-up is not complex, be patient and expect a small learning curve. Once you're up and running, this is a very user-friendly piece of kit.

The app is intuitive and the interface a pleasure to use.

For a rock-solid video doorbell camera that continues to sell out worldwide, there's no substitute for the Ring Video Doorbell. It's a classic with just cause.

Pros

- Get full HD video coverage of your home even if it's dark
- Live-View feed allows you to keep an eye on things in real time wherever you are in the world
- Alexa-enabled so you can control access with your digital assistant

Cons

- No free video storage so factor this into your budget

If you want highly effective 2-in-1 functionality, your best bet is a security camera with integrated floodlights.

Doorbell cameras are great. While they cover the entrance to your home and let you interact with visitors even if you're not at home, they also leave blind spots.

How about the drive and garden?

Dial things up and invest in a camera allowing you to monitor your home remotely while knowing it's protected by motion sensors that will trigger high-intensity floodlights and an audible alarm in the event of untoward movement being detected.

If you use Alexa, you can also control this camera using your digital assistant.

Get the full benefits of a high-definition security camera enabling two-way communication while packing floodlights and a piercing alarm.

You'll be alerted whenever the motion sensors are triggered. With a very wide coverage area and the ability to fine-tune exactly which flashpoints you want monitored, you can keep tabs on your whole property wherever you happen to me.

You can control everything from the free Ring app and use your smartphone to communicate. All you'll need is a WiFi connection.

There's a month's subscription to the video recording service so you can see whether you'd consider it worth paying for access to stored security footage.

Pros

- Enjoy clear two-way communication
- Efficient wide-angle lens offers 270 degree field of vision
- Fully customizable motion zone to highlight the most sensitive areas

Cons

Mounting plate is flimsy and requires a perfectly flat surface

You won't need to think about the expense or time of installing a full smart home security system but you can still view your home day or night in full HD.

With the best indoor security cameras, you get two-way communication so you can interact with your family, pets or visitors from your smart phone.

If you strip down the basic requirements of an effective smart home, perhaps the main objective is to be able to see what's happening even if you're not there.

With today's fluid lifestyles, frequent travel is commonplace. If you're away on business, the last thing you want to worry about is whether or not someone has broken into your house.

Functionality varies beyond monitoring live or recorded 1080 HD footage of what's happening in the protected areas. You'll sometimes get two-way audio and you can find models tailored toward monitoring your baby. More expensive models serve as a hub.

Most of the best indoor cameras connect using WiFi while some while use Z-Wave or Zigbee.

Almost without exception, you'll now be able to use your favorite digital assistant to add voice control to your smart home security.

Where Ring is the default option for many elements of home security, Nest is the go-to for indoor security cameras.

Once you've got up and running straight out the box, you'll immediately see why the Nest Cam is a global success.

Once you've got up and running straight out the box, you'll immediately see why the Nest Cam is a global success.

With alerts keeping you informed in-app and two-way audio to enable remote communication, this is a robust camera giving you complete peace of mind.

With alerts keeping you informed in-app and two-way audio to enable remote communication, this is a robust camera giving you complete peace of mind.

Cloud storage means you'll have access to footage as required without clogging up your own devices with endless bulky video files.

Keep an eye on your home round-the-clock and sleep better at night with the Nest ramping up your homes security. Explore the rest of the large Nest Family for inspiration on building out your smart home security system further.
Pros

- **Constant live streaming with Nest cam never running out of juice**

- Allows the whole family to sign in from any device
- Get alerts on your smart phone wherever you are

Cons

- Fairly expensive, especially with subscription charges

Other Outdoor Cameras

If you're looking to step up security outside, you've got a huge choice of outdoor security cameras.

Video doorbell cameras are fit for purpose but they don't do much for exposed walkways and outside spaces.

You can't just throw any old security camera outside, though. You need to make certain you get a unit that's completely weatherproofed and fit to withstand the elements.

Most outdoor cameras are fairly easy to install but you might need to call in an electrician.

You could spend years debating which outdoor security camera system was the most effective or you could save your time, bite the bullet, and invest in the Arlo Pro. It's not cheap but you'll know your garden is permanently secured and you can't really put a price on that peace of mind.

The base station provided acts as a hub and you can pop the cameras anywhere you like since they are built to cope with the elements.

Batteries are rechargeable and should give you plenty of life under normal conditions.

Video footage is detailed and 1080 HD so you can keep an eye on things from your smart phone. You can also control a 100-decibel siren remotely placing everything in the palm of your hand.

For a wireless monitoring system to help you secure your whole property, the Arlo Pro is a must.

Pros

- Crisp and clear 1080 HD video
- Completely weatherproof so put the camera wherever you want, indoors or outside
- Current version supports both Alexa and IFTTT

Cons

- Not the cheapest option but outstanding overall value

2) Door Locks

Smart door locks are a core component of any comprehensive home security system.

Using a communication protocol like **Bluetooth**, **WiFi**, or **Z-Wave**, your smart lock can communicate with other devices in your home.

Which of these works best and why?

- **Bluetooth:** With extended battery life and no need for a hub, Bluetooth makes for a seamless connection with your smart phone. On the flip side, range is sorely limited maxing out at 300 feet
- **WiFi:** Unlike Bluetooth, you'll need a separate hub like the August Connect which acts as a bridge but slacks the functionality of a multi-purpose hub.
- Z-Wave: If you opt for a smart lock using Z-Wave, you'll need a hub to translate the signal. Range tops out at 100 feet. These smart locks are ideal if you're aiming to run multiple devices in your smart home

3) Motion Sensors

Motion sensors have come a long way since the ultrasonic models of the 70s prone to false positives but setting in motion the more advanced **passive infrared (PIR) motion sensors** central to all the best smart home security systems.

Infrared has become the industry standard. Sensors detect moving objects penetrating the protective grid and the alarm is triggered.

You've got 2 choices with motion sensors:

- Indoor Motion Sensors
- Outdoor Motion Sensors

Indoor Motion Sensors

One of the leading benefits of using motion sensors indoors is the way you can have lights activated so there's no more tripping over yourself to the bathroom in the pitch black.

Since lighting is also dependent on motion being detected in each room, you'll save money on your electricity bill as an added bonus with indoor motion sensors.

You use this cost-effective indoor motion sensor along with a SkylinkHome receiver to ensure lights are activated any time motion is detected in the room. Combine convenience and economy in a pocket-friendly package.

The timer along with the motion detector hitting the lights automatically when rooms are empty means you don't need to worry about soaring electricity bills with your kids never remembering to turn off the lights.

Although the controller comes at extra cost, it's well worth the nominal investment for the added reach you'll get.

With rolling code technology minimizing any chance of a security breach, this is a strong indoor motion sensor helping you save money and detect any intruders in one hit.

Pros

- You can control a number of wireless receivers from a single sensor at ranges of 500 feet
- Use the controller to take charge of groups of lights
- Countdown timer is a nice added touch to shave even more off your utility bills

Cons

- Remote control is available at extra charge but at this price-point, you can't really complain

Outdoor Motion Sensors

Outdoor motion sensors are most frequently used together with security cameras to make sure your garden remains safe from intruders.

You'll need to pay attention to sensitivity if you don't want to enrage your neighbors with false alarms bathing the garden in light or sounding a shrill alarm every time an animal triggers the sensor.

Get the right weatherproofed system, ideally with cross-zoning to prevent the chance of improper alarm activation, and you'll sleep more soundly knowing your property is safe inside and out.

Optex delivers the full benefits of passive infrared detection technology in a scaled-down unit ideal for placing anywhere in the garden even if you live somewhere with hostile weather conditions.

If you have a larger outside space to secure, the wall-bracket offers you a 190-degree rotation so you can keep a close eye on larger gardens with ease. Select 2-meter or 5-meter detection range so a nice, flexible solution.

Since 2 zones need to be triggered, you'll get few false alarms. This is ideal if you have neighbors in close proximity.

For an extremely effective and durable outdoor motion sensor from an industry giant, the Optex FTN-ST is unbeatable.

Pros

- Outstanding wide field of vision protecting large areas with ease

- Very few occurrences of false positives whether through weather, animals, or outside events

  with 2 zones that need breaching to register positive alarm

- Fully weatherproofed and built to last for years

Cons

- Reasonably expensive

BACKGROUND AND PROBLEM STATEMENT

The default Proxy Mobile IPv6 (PMIPv6) based SH-IoT networks allow a Mobile Node (MN) to communicate with Corresponding Nodes (CNs), which are SHIoT 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 MNandMAG, 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 aMAG and aHGWto 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.

Related works

Smart home network

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 identi_ed 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 identi_ed risks. Ge *et al.* [14] developed a framework for the security evaluation of IoT devices. The authors designed a _ve-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 de_ne security framework for smart home IoT networks. The authors used software-de_ned solutions to provide a modular and _exible 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 inef_cient passage of data between mobile nodes and sensors make this solution applicable to limited scenarios.

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 theIETF [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 saf 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 SSKprotocol 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-conguring and maintenance of key materials. The TBUA protocol suffers from a major issue of security and ef_ciency 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.

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 *KLMA□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 integrity and confidentiality of the communication. This corresponds to the
security considerations defened 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 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, *KLMA□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 Difference-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.

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 Difference-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 re-establishment and performance will be evaluated using varying traffic and mobility models.