MoTH: Mobile Terminal Handover Security Protocol for HUB Switching based on 5G and Beyond (5GB) P2MP Backhaul Environment

Jiyoon Kim, *Student Member, IEEE,* Philip Virgil Astillo, Vishal Sharma, *Member, IEEE,* Nadra Guizani, and Ilsun You, *Senior Member, IEEE*

***Abstract*— With the evolution of wireless technologies, 5G and Beyond (5GB) communication is paving a way for efficient, ultra-reliable, low-latent, and high converging services for the Internet of Things (IoT). Along with efficient communication, the security of messages is one of the concerns which must be maintained throughout the operations. Backhaul forms an essential part of 5GB with an ability to enhance the coverage and quality of service for IoT. However, conventional wired backhaul connection would cost operators thousands of dollars in the construction of 5GB infrastructure considering the ultra-dense nature of IoT. As a result, wireless backhaul is quickly becoming a feasible alternative to address 5GB's direction towards network densification without affecting its other provisions. Wireless backhaul is expected to increase the landscape, covering from islands to mountains, which were difficult to access in the existing network generation. Moreover, it can effectively respond to the situation where the data traffic tremendously increased. Despite such provisioning, the wireless backhaul poses relatively various security threats and vulnerabilities due to the characteristics of wireless technologies. Several studies have been conducted to address the security problems; however, existing protocols do not support dynamic security policy and key management in a decentralized structure as well as secure handover in a specific scenario where Terminals (TMs) are moving. Motivated by this, we proposed the Mobile Terminal Handover Security Protocol (MoTH) to provide secure handover of mobile terminals between hubs. To solve the problem of existing protocols, a new entity called Backhaul Management Function (BMF) is introduced to support distributed and dynamic security policy and key management in each serving network of 5GB backhaul environment. The proposed protocol satisfies security requirements including authentication and key management, confidentiality, integrity, and perfect forward secrecy. Additionally, it supports policy and key update services, and optimized handover. The security and correctness of the proposed protocol are thoroughly verified using the two formal security analysis tools, BAN logic and Scyther. Additionally, the performance evaluation shows that the proposed protocol is efficient.**

***Index Terms*—5G and Beyond (5GB), IoT, Wireless Backhaul, Hub Switching, Handover Security, Formal Verification**

I. Introduction

THE standardization phase of 5G communication wireless system has finally reached to its conclusion. The countries leading the research on 5G technology has already started to roll-out and consequently, consumers are now gradually experiencing some of its visioned core services. Meanwhile, the most anticipated technologies that 5G wireless system is expected to support are the Internet-of-things (IoT)-based solutions for various application such as telemedicine, autonomous cars, distance education, etc. [1]. However, as the proliferation of IoT-enabled services continue, the scale of connected devices is also expected to surge up to million-fold. Consequently, the volume of data traffic generated by these devices will defeat the wireless spectral efficiency of 5G. It is estimated that traffic volume per month will reach 4394 exabytes by 2030 [2]. For this reason, academe and industry has again synergized in conceptualizing 6G wireless technology to transcend the capabilities of 5G in handling larger data capacity and lower traffic latency to a more reliable connectivity of Internet-of-Everything (IoE) [3][4][5].

Backhaul infrastructure is one essential component in the mobile cellular network as it provides a link between the base station to the core network. Point-to-Multipoint (P2MP) backhaul configuration is a serving point in the 5G set up specifically for providing new services and enabling key technologies for IT convergence [6]. To accommodate the seamless connectivity of massive IoT not only in 5G, but especially in 6G, strategical deployment of an additional backhaul is necessary while considering such configuration. In general scenarios, a wired backhaul is preferred, however, given the complexity of the urban areas and the accessibility of remote rural settlements, unconventional wireless backhaul deployment, either in static or mobile platforms, become an integral strategy both in 5G and beyond [7][8]. Logistically, wireless backhaul plays a major role in addressing key challenges under both generations in terms of flexibility, lesser effort, and rapid network establishment with great emphasis to

This work was supported by the Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. 2020-0-00952-001, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability) as well as the Soonchunhyang University Research Fund.

J. Kim, P.V. Astillo, and I. You are with the Department of Information Security Engineering, Soonchunhyang University, Asan-si 31538, South Korea (email: 74jykim@gmail.com; pvbastillo@gmail.com; ilsunu@gmail.com).

V. Sharma is with the EEECS, Queen's University Belfast, Belfast BT7 1NN, U.K. (email: vishal_sharma2012@hotmail.com).

N. Guizani is with the School of Electrical Engineering & Computer Science, Washington State University, USA (email: nadraguizani07@gmail.com).

isolated locations at an effective cost [9]. Furthermore, with the division of the network into multilayers, such as in ultra-dense networks, wireless backhaul is one of the solutions that need to be considered as well as resolve the key security issues around it [10]. With wireless backhaul, all security issues that prevail on the fronthaul security become important to manage, especially if the terminals are themselves mobile. Even if the security is provided using the existing core authentication schemes, their flexibility and adaptability along with signaling cost are major factors that affect the performance of the network [7][11][12]. With these, perfect forward secrecy during the handover, mutual authentication, handoff authentication, confidentiality, and integrity are the key security requirements of the network [13][14]. However, such provisioning is difficult to obtain as the network involves a complex architectural layout where terminals are moving, and the devices are affected by multiple key exchanges between the infrastructure itself. These types of setups need solutions with flexible security models that can adapt and coordinate their operations, such as encryption to facilitate the users with high-performance services.

There have been some works related to the backhaul security management, such as [6], [15], but the existing systems do not consider the requirement of flexible and adaptive key management along with session updates, which can elongate the security life of the network. This also saves a lot of updates which in return reduces the associated overhead on the reauthentication of the network. Additionally, some protocols are built around P2MP, which does not consider mobility management, as well as the handover of the entities and provides security in the static phase. In one of our earlier works, which provides P2MP backhaul security does not consider the handover, which is a key requirement for wireless backhaul.

In addition, existing studies did not consider the scenario of hub switching that could occur due to user movement, physical failure, or error. The proper hub switching can satisfy the availability to provide the user's continuous service in a variety of situations, from simple user movement to malicious attacks.

In an IoT-enabled smart city environment where seamless connections and secure resource sharing are steadily required, the availability that can be obtained through a hub switching scenario can be expected to dramatically increase QoE. Considering the large traffic of 5GB mobile communication, load balancing through hub switching can be applied.

With a focus on expanding the 5GB networks with wireless backhaul for IoT, it is required to consider the handover between the terminals that are operating under a HUB switching architecture. To resolve these requirements and the problem of secure handover on 5GB-based wireless P2MP backhaul, the following contributions are obtained in this paper:

1. A secure terminal handover protocol with P2MP backhaul setup over 5GB is proposed that uses the security functions for improved mobility control.
2. The protocol considers a scenario of hub switching focusing on the properties of authentication, confidentiality, integrity, secure key exchange, and perfect forward secrecy, all of which are bundled with a key concept of adaptive and flexible security provision through policy update phase.
3. The advantages of the proposed protocol, Mobile Terminal Handover (MoTH) are demonstrated in terms of security advantages using BAN logic and Scyther tool.
4. Comparison with one of our recently proposed protocol for P2MP backhaul security (Kim et al. [6]) as well as a host-based backhaul handover mechanism (Sharma et al. [15]) are provided in terms of computational overheads, signaling overheads and handover latency.

The rest of the paper is structured as follows: Section II presents the related works, Section III gives the details of the proposed protocol, Section IV provides the formal analysis of the proposed protocol. Numerical evaluations are presented in Section V. Finally, Section VI concludes the article with highlights of the future works.

II. Related works

Backhaul is a key part for extending the network which aims to the densification of services as well as infrastructure. It covers the link to the core of the network and plays a significant role in the efficient management of the entire network. In general, backhaul is operated through a wired medium, however, most recently with the extension of 5G non-standalone architecture, wireless backhaul has been a key area of focus to enhance the capabilities of the network. In particular, the use of mm Wave technologies has been the recent area to target for efficient backhaul management. However, despite several studies on the efficiency of backhaul, very limited has focused on the handover management considering that the entire system has a moving fronthaul and the connectivity between the backhaul and the core is based on the mobile entities. Some of the protocols that can ensure the security of the backhaul includes, Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) [16], Transport Layer Security (TLS) [17], Internet Key Exchange Mobility and Multihoming (IKEv2) [18], Host Identity Protocol (HIP) [19] and Point to Multi-point (P2MP) [6]. For these protocols, only P2MP has provided evident support for covering backhaul security, which forms the basis of the proposed protocol, however, in the current form, it cannot ensure the handover management, and it lacks backhaul management for supporting mobile terminals[1].

Apart from these, certain articles studied the mobility management of backhaul networks with and without the focus on security. However, these articles are not particularly focused on backhaul security and mobility management across it. Sharma et al. [15] considered a 5G-Xhaul scenario which included mobile TMs. The authors used Diffie-Hellman key exchange as a key operation for securing the handover operations. However, this protocol is host-initiated, which offers lower control to the network when the backhaul is involved. Moreover, under the P2MP single-relay scenario, the

[1] This work is an extension of our earlier version of P2MP protocol, which is improved to support mobility management for TMs under backhaul scenario by considering a dedicated backhaul management function.

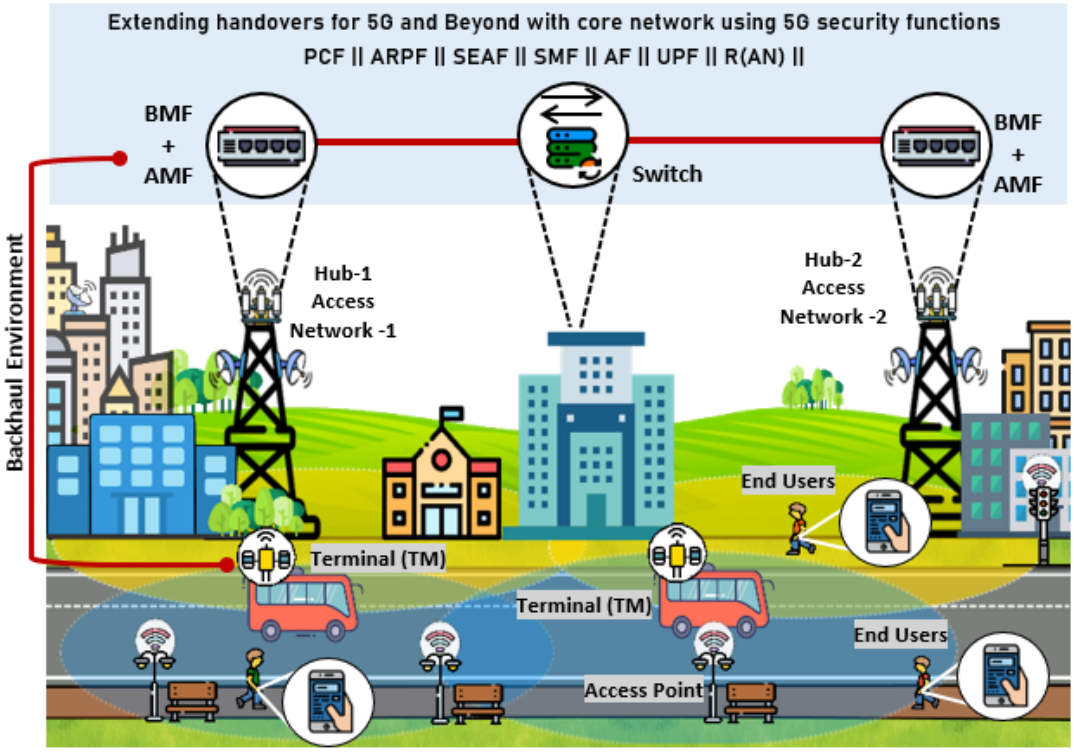

Fig. 1. An IoT Network using 5GB wireless backhaul scenario for handover management.

performance of the protocol degrades, which should not happen as backhaul relies on such setup for communications.

Liyanage et al. [20] emphasized LTE-Backhaul security and provided different challenges associated with the security of backhaul traffic. The authors considered a fixed terminal LTE setup and discussed security issues around trusted domain-based and IPsec VPN-based backhaul architectures.

Kaloxylos et al. [21] focused on the session and mobility management in SDN-enabled 5G networks. The authors explored the 5G security functions of the 3GPP and suggested the methodologies for including SDN in 5G to increase the performance in the densification of the network.

Advantages of optimal security management can be followed in Sharma et al. [22]. The authors studied the current 5G security functions and discussed optimization problems associated with the key management and presented a study on the enhancement of security by having a flexible key update mechanism. The authors provided an evaluation on the identification of fail-safe points after which the keys should be updated to keep the network secure, especially targeting the backhaul of 5G networks. The authors used the vehicular setup as the end device and proposed a subdivision of the keys to bring security anchor functions near to the user to improve the overall performance of the network. However, the detailed security requirements and properties of handovers are not studied in this article.

Efficient mobility management is affected by joint access and backhaul optimization as studied by Rony et al. [23]. The authors presented a brief study on backhaul and fronthaul considering the futuristic 5G scenarios. However, the study does not consider the evolution of the mobile fronthaul or backhaul for enhancing the performance as well as the types of services over 5G networks. Hu et al. [24] focused on the integration of Media Independent Handover (MIH) and Software Defined Networks (SDN) for mobile backhaul systems. The approach used in their work relies on a preselection scheme to eliminate unqualified networks and generate a network ranking for efficient handover. The work is around the selection of optimal network in case multiple access technologies are available in the setup. Similar understanding can be followed in MIH-integrated setup studied in [25], which includes the integration of Fast-Proxy IPv6 with MIH to have efficient and media-independent mobility management.

In another article, Sharma et al. in [26], the authors proposed a secure protocol for distributed mobility management using blockchain. The authors considered network flattening a driving factor for proposing a security protocol. Although the protocol is secure, its performance is governed by the principles of the blockchain, which itself is slow to converge, and causes much consumption of resources. From the literature presented in this section, it can be summarized that backhaul security considering the mobile terminals is important, but none of the existing articles considers a network-initiated solution which not only enhances the security and does not compromise with the performance of the network.

III. Proposed Protocol

This section describes the details of the proposed protocol and encryption process. The proposed protocol provides the security of the 5GB wireless P2MP backhaul handover which is practical for ultra-dense scenarios related to IoT. The target environment of the proposed protocol is composed of terminal, hub, backhaul management function, and authentication server function, which are denoted as Terminal (TM), hub (HUB), Backhaul

Management Function (BMF), and Authentication Server Function (AS), respectively.

The protocol consists of three phases, Init phase, Policy Update phase (PU phase), and Handover phase (HO Phase). The complex network such as the target environment, mixed with TM and HUBs, needs to utilize the policy for efficient management. For this, the proposed protocol can update the policy with the PU phase when the network situation changed.

The wireless-backhaul handover protocol, depicted in Fig. 1, is considered for hub switching scenario based on 5GB networks. The HUB switching can happen when the mobile device that was attached to the previous HUB moves to the area of the new HUB. In this case, HO phase is needed. The HO phase can provide a secure and fast handover between TM and HUBs.

In addition, the session keys are exchanged between TM and HUB by the ECDHE (Elliptic Curve Diffie-Hellman Ephemeral). Generally, the ECDHE has fewer resources and key values, but is known to be safer than the general Diffie-Hellman. And the ECDHE can provide the perfect forward secrecy with the ephemeral characteristic that destroys the key derived in the Diffie-Hellman step after a specific encryption operation required and creates a new key again when it necessary.

A. Assumptions and Security Requirements

Table I shows the notations used in this paper and its meaning.

TABLE I
NOTATIONS

Notation	Meaning
TM	Terminal
pHUB	Previous Hub
nHUB	New Hub
BMF	Backhaul Management Function
ASF	Authentication Server Function
PU	Policy Update
HO	Handover
ID_X	X's identifier
Capability	List of the available cryptographic algorithms, methods of authentication and key exchange, etc.
Policy	The selected methods from Capability
K_{X-Y}	Pre-shared key between X and Y
PMK	Pre-Master Key
MK	Master Key
AK	Authentication Key
CK	Cipher Key
K_{old}	Secret key of previous session
CM	AES128-CMAC
ts	Timestamp
nx	x-th nonce

The assumptions made on the proposed protocol are as follows:

- It is assumed that a secret key $K_{TM, ASF}$ and the identifier of TM, ID_{TM} are shared between TM and ASF.
- It is considered that the secure channels are formed by using the own shared key between pHUB, nHUB, BMF, and ASF.
- BMF generates the policy that contains the network state, the key exchange information, and the encryption strength.

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

- **Mutual authentication:** During the process, the communication participants should mutually authenticate each other.
- **Confidentiality:** Any unauthorized participants should not be able to read transmitted messages between authorized users.
- **Integrity:** Any unauthorized participants should not be able to change the transmitted messages between authorized users.
- **Secure key exchange:** After the process, both participants should negotiate the authentication key and the cipher key.
- **Perfect Forward Secrecy:** The current session key should not be derived in any way from the past one.

B. Proposed protocol

The proposed protocol consists of three phases: Init phase, PU phase, and HO phase.

1) Init Phase

In the first step, TM must authenticate with HUB and ASF to gain access to the network. Fig. 2 illustrates the authentication process of TM. The detailed descriptions of the protocol are as follows:

1. At the first connection of TM to the network, it sends the Auth_Req message to HUB. The message contains IDs of TM and HUB, freshly generated timestamp (ts) and nonce (n1), TM's security capability, and CMAC value CM1. The CM1 value, which is calculated using MK, provides the authenticity and integrity of the message. Upon reception, the HUB forwards the Auth_Req message through BMF to ASF for authentication. When ASF receives the message, it first validates the timestamp (ts) if valid. If the timestamp (ts) is valid, ASF calculates the PMK with the shared secret ($K_{TM, ASF}$) and the received timestamp value. Subsequently, it derives MK from PMK as well as ts. Thereafter, ASF can verify the authenticity of Auth_Req message using CM1. If verification is valid, subsequent steps are performed.

2-a. ASF responds to the request by sending ASF_Auth_Res message that contains the pre-master key (PMK) to BMF over a secure channel.

2-b. Upon reception of ASF_Auth_Res, BMF calculates the master key (MK) using the received pre-master key (PMK) and timestamp. It also generates the policy according to the network condition and performance of each devices. Thereafter, it forwards the ASF_Auth_Res message to HUB, but the content is replaced by the generated policy together with MK.

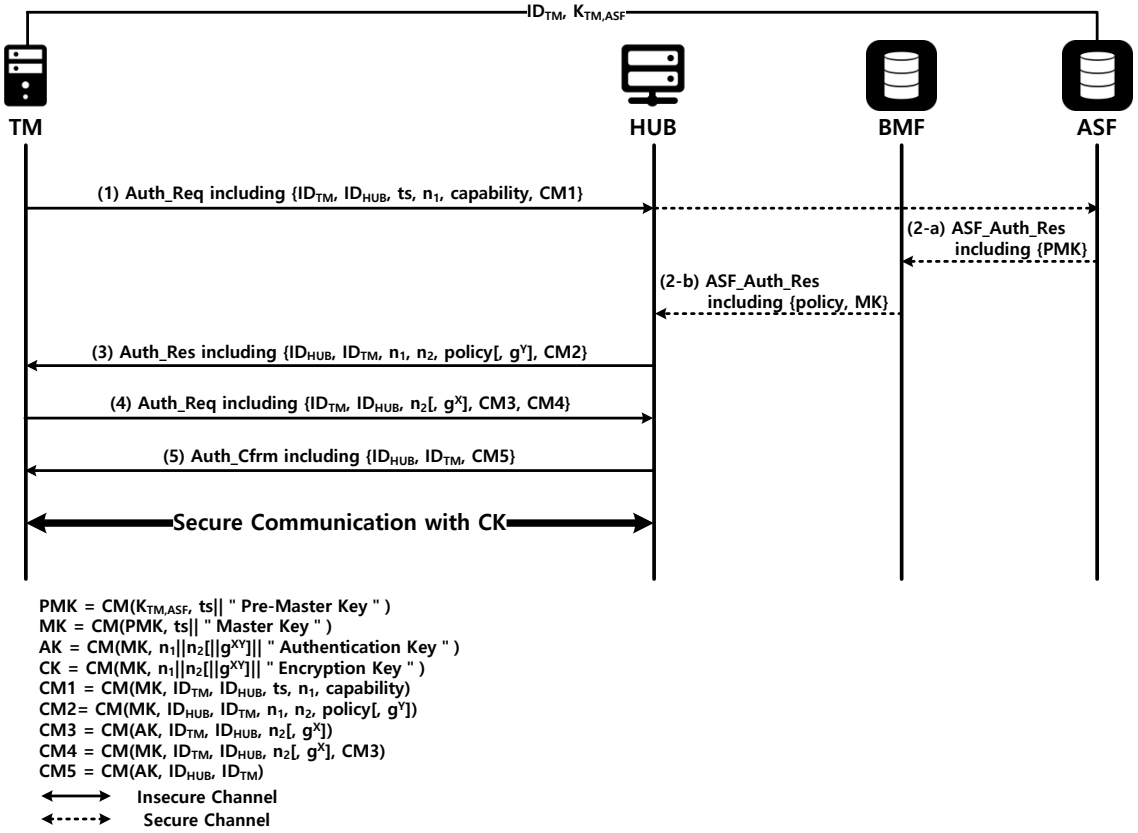

Fig. 2. Init phase of the proposed protocol

3. Upon receiving the ASF_Auth_Res message, HUB sends the Auth_Res message that includes the IDs of HUB and TM (IDHUB, IDTM), the nonce received in step 1 (n1), the freshly generated nonce (n2), the policy, and an optional Diffie Hellman public key (g^Y). The inclusion of the Diffie-Hellman public key depends on the policy provided by the ASF. Additionally, CMAC (CM2) value over the message is calculated using MK and included to protect it. Subsequently, upon receiving the message, TM checks the message's freshness by n1 and verifies it through CM2. If the verification is valid, TM generates an authentication key AK and an encryption key CK using MK, the two nonces n1 and n2, and the Diffie-Hellman key g^{XY}, if suggested in the policy. TM will then send its response to HUB.

4. TM will respond depending on the received policy. It sends the Auth_Req message together with the IDs (IDTM, IDHUB), the nonce received in step 3 (n2), and an optional Diffie-Hellman public key (g^X) to HUB. The Auth_Req message is protected by two CMACs CM3 and CM4. CM3 and CM4 are calculated using MK and the generated authentication key AK, respectively. Once this message is received by HUB, it will first verify the authenticity of the message by validating CM4. A valid result implies that the message can be trusted for coming from a legitimate TM. Additionally, HUB can establish trust with TM by having the same MK. In such case, the HUB subsequently verifies the received CM3. It validates the received CM3 by generating an authentication key AK and use it to compute the CMAC value of the message's plaintext fields. A positive comparison between the received CM3 and the computed value implies that the HUB can trust TM of having the same AK. If all validation is successful, the HUB responds with a confirm message to TM.

2) Policy Update Phase

The generated policy contains information of the network requirements which may include traffic capacity, transmission latency, security, supported cryptographic algorithms, and key exchange mechanisms. Policy update is initiated in situations where the encryption method must be strengthened or slightly relaxed in response to the network condition, or the key lifetime has expired. BMF monitors the network condition and decides if the policy needs an update or not. Fig. 3 illustrates the policy update phase, and the detailed descriptions are as follows:

1. If BMF decides to update the policy in response to the network condition, it sends PU_Init message to the HUB over the secure channel. The parameters included in this message are the fresh timestamp and master key MK, as well as the new policy.

2. Upon receiving the PU_Init message, the HUB generates the new authentication parameters such as the nonce (n1) and optional Diffie-Hellman public key (g^Y). These parameters, along with IDs of HUB and TM, the received ts, and the new policy are sent to TM in a PU_Req message. Additionally, CMAC value CM1 is included to protect the message. Once TM receives the message, it first checks the timestamp ts if it is

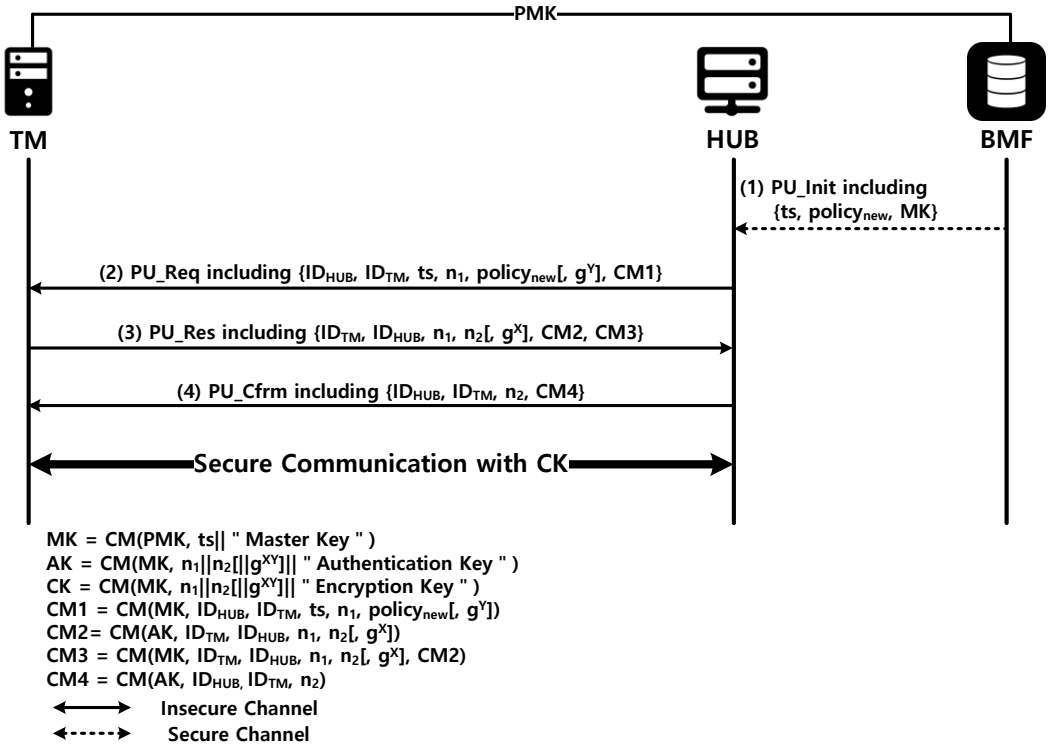

Fig. 3. Policy update phase of the proposed protocol

within a predefined range. In the positive case, TM verifies the authenticity of the message through CM1. If CM1 is valid, it will prepare its response to HUB.

3. Accordingly, TM generates the authentication parameters such as the nonce (n2) and an optional Diffie-Hellman public key (g^X) in accordance with the new policy. TM responds to the HUB with the PU_Res message that contains HUB's and TM's IDs, the authentication parameters, and two CMAC values CM2 and CM3. CM2 and CM3 are sequentially calculated using the new authentication key AK and master key MK, respectively. Upon reception, the HUB verifies the integrity of message through CM3. In positive cases, it also validates CM2. If the validation is successful, the HUB can trust TM of having the same MK and AK. Accordingly, the HUB confirms the policy update and the generation of new session keys.

4. HUB confirms by sending PU_Cfrm message to TM together with HUB's and TM's identifier, and the received nonce n2. In addition, CMAC CM4, which is generated using AK, is included to protect the message. Upon receiving the message, TM checks the received nonce n2 if it is the same with the one sent by it in the previous message. Subsequently, it verifies the message through CM4. In positive verification, TM could trust HUB for having the same AK. Additionally, this means that the policy update was successfully carried out.

3) Handover Phase

This paper considers TM to be mobile, hence it can transfer the connection from one HUB to another. In such scenario, the security context must be transferred from the previous HUB (pHUB) to the new HUB (nHUB). Figure 4 illustrates the process for the handover and the detailed descriptions are as follows:

0. The pHUB monitors the movement of TM. In case TM needs to transfer its point of attachment, the pHUB reports to BMF by transmitting the HO_Trigger message. Every time BMF receives a HO_Trigger message, it will initiate the handover procedures.

1. BMF prepares HO_Init message and transmits it to HUBs involved in the handover. The content of the message differs for each recipient. BMF sends the HO_Init message to the pHUB including the IDs of handover participants (TM, pHUB, nHUB), and the timestamp (ts), the new policy ($policy_{new}$). On the other hand, the HO_Init message intended for nHUB includes the IDs of handover participants (TM, pHUB, nHUB), and the new policy ($policy_{new}$), and the master key (MK). In this time, both HUBs can configure the channel for data transfer. This channel can provide the continuity of the data transmission.

2. After channel configuration, pHUB sends the HO_CMD message, excluding the ID of pHUB (ID_{pHUB}) from the HO_Init message to TM. This message is protected by CMAC (CM1). When TM receives the HO_CMD message, TM can verify the CM1 via the master key MK_{old} which is shared between TM and pHUB at the last session. If the verification of CM1 is positive, TM will prepare the handover request message.

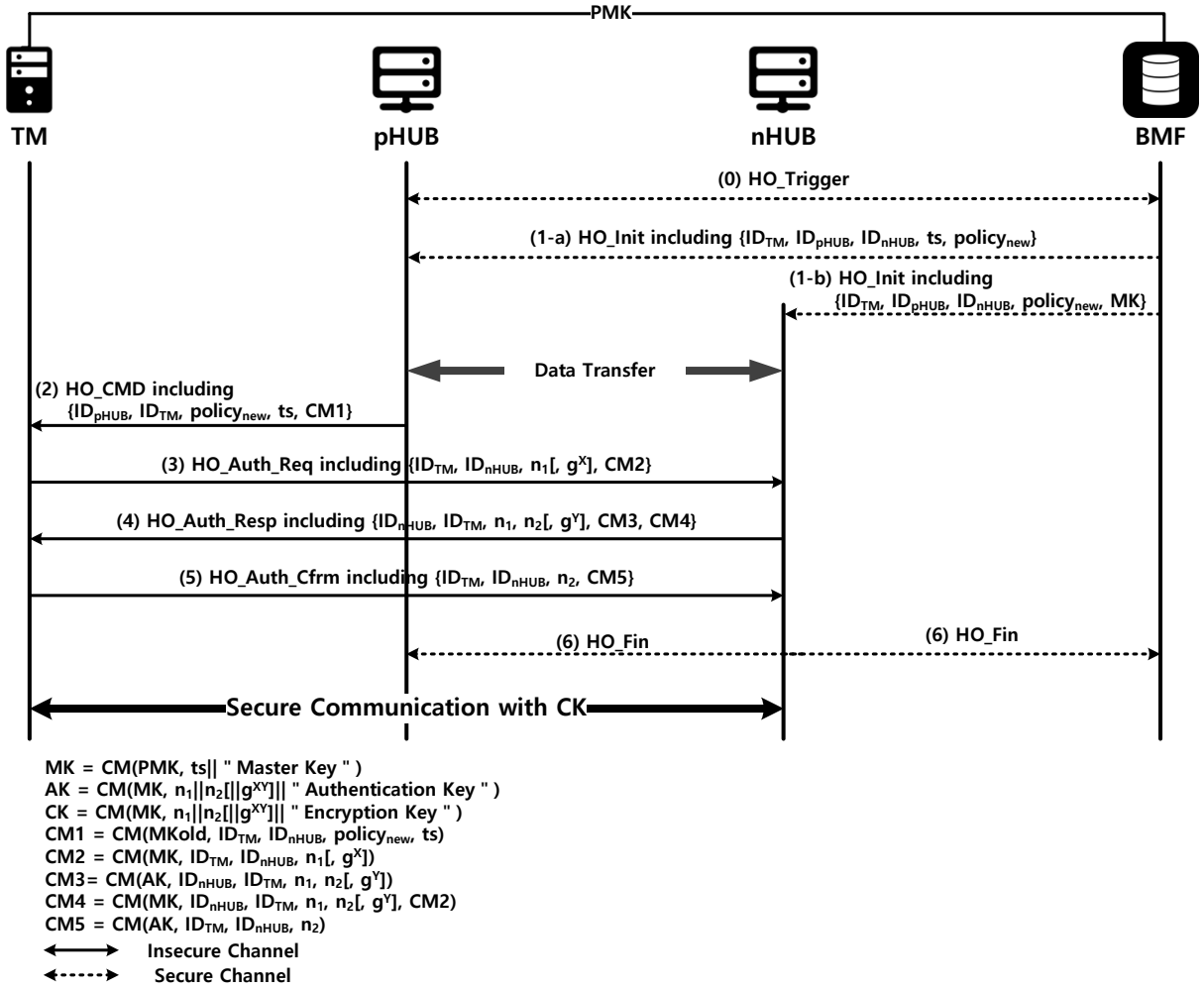

Fig. 4. Handover phase of the proposed protocol

3. The preparation of the request message HO_Auth_Req is based on the received new policy from pHUB. Accordingly, TM may include a Diffie-Hellman public key (g^X) together with freshly generated nonce n1, TM's and nHUB's identifiers in the message. It is also accompanied with CMAC CM2 for protection. Subsequently, the HO_Auth_Req message is transmitted to nHUB. Once this message is received by nHUB, it first validates CM2 using MK and responds to TM if valid. In such case, nHUB can trust that TM has the same master key MK.

4. In response to the HO_Auth_Req message, nHUB sends the HO_Auth_Resp message to TM, which includes the IDs of nHUB and TM, the received nonce n1 from previous messages, generated nonce n2, and an optional Diffie-Hellman public key (g^Y). Additionally, HO_Auth_Resp message is protected by two CMAC CM3 and CM4. Upon reception, TM verifies CM using the new MK. The message is trustworthy if the validation is positive. Thereafter, TM also verifies CM3 using an authentication key AK. In case of positive result, TM can now trust nHUB of having same AK and confirm with nHUB.

5. TM confirms the key exchange during handover by sending the HO_Auth_Cfrm message. The message contains the IDs of TM and nHUB (IDTM, ID_{nHUB}), the received nonce n2, and protected by CMAC value CM5. Subsequently, once nHUB receives the confirmation message, it validates its integrity using AK. If the validation is successfully, nHUB can fully trust TM. In addition, the positive result implies that the two parties must mutually authenticate each other and successfully exchange session keys.

6. Finally, nHUB sends the HO_Fin message to pHUB and BMF to inform them that the handover procedure, authentication, and key exchange were successful.

IV. Formal Verification

This section aims to the formal verification of the proposed protocol. In this case, the proposed protocol is verified through two widely applied tools: BAN logic [27] [28] and Scyther [29]. Using these tools, the proposed protocol can prove its safety. The BAN logic's equations are provided at the end of the paper in APPENDIXs. Also, the results and codes for Scyther are provided as separate files.

A. Formal verification with BAN logic

BAN logic, introduced by Burrows, Abadi, and Needham, is a set of rules for verifying the target protocols. The formal

TABLE II
BASIC NOTATIONS OF BAN LOGIC

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

TABLE III
RULES OF BAN LOGIC

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

verification with BAN logic is composed of three steps: (1) idealization, (2) assumption and goal, (3) derivation. For accurate verification, the BAN logic provides basic notations and rules as shown in Table II and Table III.

1) Init Phase

In the first step, the Init phase is idealized as shown in Equation 1 of APPENDIX A. Based on the idealization, the assumptions and goals are made and defined as shown in Equations 2 and 3 of APPENDIX A. The goals, (GI1) and (GI2) mean that the status information of network and device is exchanged securely. And (GI3) and (GI6) mean that the master key (MK) is securely distributed by BMF. Finally, (GI4) -(GI5) and (GI7) -(GI12) indicate that the authentication key AK and the cipher key CK are successfully exchanged between TM and HUB.

From the derivations (D1) -(D29), the Init phase achieves the goals (GI1) -(GI13). By the achieved goals, we can obtain the following lemmas:

Theorem 1: The Init phase of the proposed protocol is secure.

Lemma 1-1: The Init phase of the proposed protocol can provide mutual authentication.

Proof: The derived beliefs (D8) and (D16) show that both TM and HUB have mutually authenticated each other. Moreover, from the belief (D4), the TM authenticates to the serving networks. Therefore, it can show that the Init phase provides mutual authentication stronger. □

Lemma 1-2: The authentication key AK and the cipher key CK are successfully exchanged between TM and HUB.

Proof: TM can believe AK and CK through the derived beliefs (D11) and (D12). On the other hand, HUB can believe the AK and CK through (D19) and (D20). However, these beliefs indicate that believe the key itself. The derived beliefs, (D23) -(D24) and (D28) -(D29), show that the indirect beliefs on AK and CK. By direct and indirect beliefs, we can show that the authentication key AK and the cipher key CK are successfully exchanged between TM and HUB. □

Lemma 1-3: The Init phase of the proposed protocol provides the perfect forward secrecy.

Proof: From (D10) and (D18), TM and HUB are exchanged for the Diffie-Hellman session key g^{XY} by the ECDHE procedure. After these procedures, both participants remove their own private key. Therefore, the session key cannot be recovered, even other keys are exposed. In conclusion, the Init phase of the proposed protocol can provide the perfect forward secrecy. □

Lemma 1-4: The Init phase of the proposed protocol can provide confidentiality and integrity.

Proof: The meaning of confidentiality represents that the message exchange performs based on the secure key exchange and the key security. The secure key exchange can be proved through Lemma 1-2. And the Init phase can provide the perfect forward secrecy through Lemma 1-3. On the other hand, integrity indicates that the message has not been altered. From (AI3) and (AI6), both TM and HUB believe the master key MK, and they can believe that the other believes the master key MK from (D9) and (D17). □

2) Policy Update Phase

The policy update phase of the proposed protocol is idealized as shown in Equation 4 of APPENDIX B. In addition,

assumptions and goals are made and defined as shown in Equations 5 and 6 of APPENDIX B.

In Equation 6, the goals of the Policy Update phase are defined. The policy is the information on the network situation. By (GP1), the policy can be updated successfully. (GP2) and (GP5) are aims that the master key MK is securely distributed. Finally, (GP3) -(GP4) and (GP6) -(GP11) indicate that the authentication key AK and the cipher key CK have been securely exchanged between TM and HUB.

Based on the derivations, the goals defined as Equation 6 have been achieved. It means that the Policy Update phase of the proposed protocol is safe. Moreover, we can prove its safety through the following theorem and lemmas:

Theorem 2: The Policy Update phase of the proposed protocol is secure.

Lemma 2-1: The Policy Update phase of the proposed protocol can provide mutual authentication.

Proof: The derived beliefs, (D29) and (D37), show that both MN and HUB have mutually authenticated each other with MK. MN can generate MK when MN gets a valid timestamp. And HUB receives MK from BMF securely. □

Lemma 2-2: The authentication key AK and the cipher key CK are successfully exchanged between TM and HUB.

Proof: TM can believe AK and CK through (D34) -(D35). Additionally, HUB can believe AK and CK through (D41) -(D42). From (D45) -(D46) and (D50) -(D51), these show that the indirect beliefs about AK and CK between TM and HUB. By the direct and indirect beliefs, we can obtain that the authentication key AK and the cipher key CK are successfully exchanged between TM and HUB. □

Lemma 2-3: The Policy Update phase of the proposed protocol can provide the perfect forward secrecy.

Proof: The perfect forward secrecy is one of the most important security requirements of the security protocol. It can protect the key from leaking. In this case, TM and HUB are exchanged for the ECDHE session key g^{XY} as (D33) and (D40). When they generate the ECDHE session key, both of participant remove their own private key. Without both private keys, the session cannot be recovered. As a result, the session key has no relationship with the previous one. □

Lemma 2-4: The Policy Update phase of the proposed protocol can provide confidentiality and integrity.

Proof: The confidentiality can be provided when secure key exchange and key safety are guaranteed. In our case, the secure key exchange can cover by Lemma 2-2. Furthermore, the key safety can cover by Lemma 2-3. On the other hand, integrity can be provided when the transmitted message should not be altered. Based on (D30), (D38), and (D49), the receiver can believe that the transmitted message is valid. Finally, we can show that the Policy Update phase of the proposed protocol can provide confidentiality and integrity. □

As a result, the safety of the Policy Update phase of the proposed protocol (Theorem 2) can be demonstrated from Lemma 2-1 to Lemma 2-4.

3) Handover Phase

In the first step, the Handover phase is idealized as shown in Equation 7 of APPENDIX C. Based on the protocol assumptions and the security requirements, assumptions and goals are defined as shown in Equations 8 and 9 of APPENDIX C.

The goal (GH1) is related to transmit valid network status. In (GH2) and (GH5), the goals indicate the direct belief of the key distributed through BMF, and it can prove the integrity of the transmitted message. (GH3) -(GH4) and (GH6) -(GH7) are indicated direct beliefs of the participant about the keys AK and CK. In contrast, (GH8) -(GH11) represent the indirect beliefs of the participants in the keys AK and CK.

According to the derivation, we can derive the defined goals in Equation 9 and can be summarized as the following theorem and lemmas.

Theorem 3: The Handover phase of the proposed protocol is secure.

Lemma 3-1: The Handover phase of the proposed protocol can provide mutual authentication.

Proof: From (D57) and (D64), we can obtain that both MN and nHUB can mutually authenticate each other with MK. With MK, both participants can believe that the message is sent from another participant. □

Lemma 3-2: The Handover phase of the proposed protocol can provide secure key exchange between TM and nHUB.

Proof: From the derivation, (D61) -(D62) and (D77) -(D78), we can prove that nHUB believes in AK and CK directly or indirectly. Furthermore, the derivations (D68) -(D69) and (D72) -(D73), indicate that TM believes AK and CK directly or indirectly. Through this, the Handover phase can support secure key exchange. □

Lemma 3-3: The Handover phase of the proposed protocol can provide the perfect forward secrecy.

Proof: The authentication key AK and the cipher key CK are used to protect the messages exchanged between MN and nHUB. The perfect forward secrecy prevents the current key from being restored due to the key leak in the previous sessions. In every session, both participants randomly generate the ECDHE private key and discard it immediately after use. From (D60) and (D67), the authentication key AK and the cipher key CK are safe due to derived from g^{XY}. □

Lemma 3-4: The Handover phase of the proposed protocol can provide confidentiality and integrity.

Proof: The confidentiality of Handover phase can be derived through the secure key exchange proved by Lemma 3-2 and the perfect forward secrecy proved by Lemma 3-3. On the other

hand, the integrity of Handover phase can be shown through derivation of the transmitted message as in (D58), (D65), and (D76). □

As in Theorem 3, the Handover phase of the proposed protocol is secure. It can be demonstrated by Lemma 3-1 to Lemma 3-4 described above.

Finally, the results from Theorem 1 to Theorem 3 indicate that the proposed protocol can be secured through BAN logic.

B. *Formal verification with Scyther*

To strengthen the claims on the security of the protocol in the initial, policy-update and handover phases, Scyther was used for the formal verification as it helps to overcome the problems associated with the BAN logic [30]. It can support automated verification of the target protocol. The verification of Scyther is composed of three steps: (1) modeling, (2) verification, and (3) result. First, the target protocol must be modeled by the unique script of Scyther SPDL (Security Protocol Description Language). With the model of the target protocol, Scyther performs verification automatically and shows the results of the claim events. If the attack is found, Scyther shows the attack flow. The formal verification with Scyther must include the claim events. Claim events can support the checking about security properties such as authentication and secrecy. The details of claim events are available in [31]. For the formal verification of Scyther, we create and simulate protocol models for each phase of the proposed protocol. As a result, the statuses of all claim events are OK, and it shows that the proposed protocol is secure that secrecy as well as authentication. The verification results and its source codes of the proposed protocol are included in SUPPLEMENTARY FILE.

V. Comparative Analysis

In this section, the proposed protocol is compared with the core security protocols (EAP-AKA [16], EAP-TLS [17], EAP-IKEv2 [18], HIP [19] and our earlier work P2MP [6]). According to Table IV, we can see that EAP-AKA and EAP-TLS do not support perfect forward secrecy. Moreover, policy update is only supported by P2MP and MoTH, while EAP-TLS, EAP-IKEv2, and HIP are failed to support against resource exhaustion attack. The optimized handover is only supported by MoTH. As a result, only the proposed protocol MoTH can support all the security properties. In addition, the proposed protocol is evaluated for computational overhead with the security protocols mentioned in Table IV. From Table V, it is observed that the computational overhead of the proposed protocol is better than EAP-TLS and EAP-IKEv2. In case of EAP-AKA, it seems to have less computational overhead than others, but it fails to support the required security properties such as perfect forward secrecy policy update, and optimized handover.

These comparisons suggest that the proposed protocol can provide efficient and secure handover in the backhaul scenario without excessive iterations of the security messages. In particular, the efficiency of the proposed protocol is suitable for IoT environments that is sensitive to resource consumption. The existing protocols used for comparison are usually modified to support handover, however, there are no evident studies available that have used these protocols for backhaul handover management. EAP-AKA if extended with proper security mechanisms, can be a useful candidate for handover management in backhaul. However, in the current form, there are several issues related to policy update, flexible handover management, TM attack resistance, and perfect forward secrecy, which are missing in its basic form [6].

To further understand the importance of the proposed protocol, we compared it for signaling overheads and handover latency in comparison with Sharma et al.'s protocol [15] which considers mobile terminals along with a user movement like a smart city setup. With a similar architecture, the protocol is a good match to the scenario and shares a clear consideration for showing performance comparisons. For evaluations, we relied on the methodologies of protocol evaluation presented in [32], [33], [34]. In the proposed protocol, the handover phase is used for these evaluations. In the given model, the signaling overheads with mobile terminals across the hub are given as:

TABLE IV
Comparison of Protocols by Security Property

Security Property	EAP-AKA	EAP-TLS	EAP-IKEv2	HIP	P2MP	MoTH
SP1	O	O	O	O	O	O
SP2	O	O	O	O	O	O
SP3	O	O	O	O	O	O
SP4	O	O	O	O	O	O
SP5	X	X	O	O	O	O
SP6	X	X	X	X	O	O
SP7	O	X	X	X	O	O
SP8	X	X	X	X	X	O

SP1: Confidentiality, SP2: Integrity, SP3: Mutual authentication, SP4: Key exchange, SP5: Perfect forward secrecy, SP6: Policy update, SP7: Defense against resource exhaustion attack, SP8: Optimized Handover
O: Support, X: Not support

TABLE V
Computational Overheads of Different Protocols in Comparison with the Proposed Protocol (MoTH)

Protocols	**Computational Overheads**			
	TM	HUB	BMF	ASF
EAP-AKA [9] [17]	$9C_5$	-	-	$9C_5$
EAP-TLS [9] [18]	$1C_2 + 1C_6 + 4C_5 + 2C_1$	-	-	$1C_2 + 1C_5 + 1C_1 + 1C_4 + 1C_3$
EAP-IKEv2 [9] [19]	$3C_1 + 1C_8 + 1C_6 + 1C_3 + 1C_4 + 1C_5$	-	-	$3C_1 + 1C_8 + 1C_6 + 1C_3 + 1C_4 + 1C_5$
HIP [9] [20]	$1C_7 + 1C_4 + 1C_8 + 1C_3 + 1C_1 + 1C_5$	$1C_4 + 1C_8 + 1C_3 + 1C_1 + 1C_5$	-	-
*P2MP [9]	$8C_5 + 1C_8$	$6C_5 + 1C_8$	-	$2C_5$
*MoTH (Non-handover)	$6C_5 + 1C_8$	$4C_5 + 1C_8$	$2C_5$	$1C_5$
*MoTH (Handover)	$2C_5 + 1C_{8**}$	$6C_5 + 1C_{8**}$	$3C_5$	-
MoTH Total	$7C_5 + 2C_8$	$10C_5 + 2C_8$	$5C_5$	$1C_5$

C_1: symmetric encryption/decryption overheads, C_2: asymmetric encryption/decryption overheads, C_3: digital signature overheads, C_4: signature validation overheads, C_5: one-way HMAC overheads, C_6: certificate validation overheads, C_7: puzzle–cryptographic challenge overheads, C_8: Diffie-Hellman operational overheads (*Only initial phase Diffie-Hellman is evaluated; and handover includes both previous and new hubs; ** can be skipped in the handover phase).

$$S_o = \frac{Pr[F]}{1-Pr[F]} (4\, H_{TM-Hub}\, M) + (H_{Hub-Hub}\, M) + (5\, H_{Hub-BMF}\, M), \quad (5.1)$$

where ***Pr[F]*** is the probability of failure of links between the TM and the nearest serving hub, ***M*** is the message size for the transmission, and $H_{<entity>}$ is the number of hops between the involved parties. Furthermore, the handover latency is dependent on the time delay associated with the computational overheads for the involved entities. In the proposed protocol, the major role players for the handover are the TM itself, followed by the pHub and BMF, whereas nHub is majorly responsible for the confirmation procedures. Now, considering the wireless linked backhaul with layer-2 delay (α) and the time to acquire the first signal (β), the handover latency of MoTH is given by:

$$H_L = 4\, T_{TM-Hub} + T_{Hub-Hub} + 4\, T_{Hub-BMF} + I_{TM-ASF} + \alpha + \beta, \quad (5.2)$$

where $I_{TM-ASF} = 4\, T_{TM-Hub} + T_{Hub-BMF} + T_{Hub-ASF} + T_{BMF-ASF}$. Here, $T_{<entity>}$ is the associated delay in communication between the involved parties and I_{TM-ASF} is the communication overheads of the initial phase which takes place every time a TM boots or moves to the periphery of the new hub. Alongside this, the handover failure probability can be used to understand the extent of dependability of the protocol on the TM. Using the derivation in [32], the reliability of the handover can be expressed as:

$$R_F = 1 - \frac{\mu E[H_L]}{1+\mu E[H_L]}, \quad (5.3)$$

where $\mu = \frac{2V}{\pi R}$. Here, *V* is the average speed of the TM, *R* is the network coverage area for the hub and $\frac{\mu E[H_L]}{1+\mu E[H_L]}$ is the failure probability of the handover [32][33]. To follow the exact evaluations, we used common numerical simulations to analyze the performance of the proposed protocol and the existing protocol for Xhaul (backhaul part only) security as in Sharma et al. [15]. The numerical parameters used for the evaluations are given in Table VI.

TABLE VI
NUMERICAL CONFIGURATIONS [15][32][34]

Parameter	Value
M	66 bytes – 128 bytes
H_{TM-Hub} **(single-relay, multi-relay)**	1, 1
$H_{Hub-Hub}$ **(single-relay, multi-relay)**	1, 1
$H_{Hub-BMF}$ **(single-relay, multi-relay)**	1, 9
H_{TM-BMF} **(single-relay, multi-relay)**	2, 11
H_{TM-ASF} **(single-relay, multi-relay)**	3, 12
α	45.35 ms
β	10 ms to 50 ms
Pr[F]	0.1 to 0.5
T_{TM-Hub}	20 ms
$T_{Hub-BMF}$	$H_{Hub-BMF}$. 20 ms
$T_{Hub-Hub}$	$\sqrt{T_{Hub-BMF}}$
$T_{BMF-ASF}$	20 ms
T_{TM-ASF}	$H_{TM-ASF} . T_{TM-Hub}$
$T_{Hub-ASF}$	$(H_{Hub-BMF} + 1)$. 20 ms
V	10 m/s-15 m/s
R	200-400 m

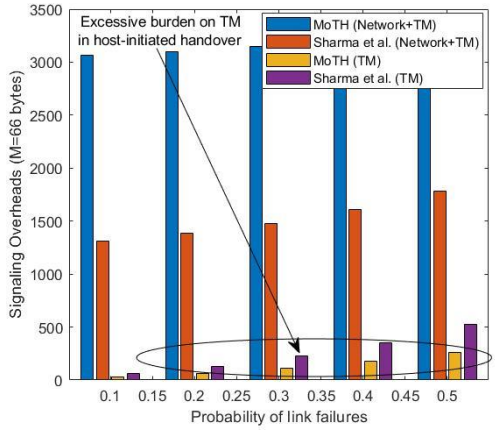

Fig. 5. Signaling overhead vs. probability of link failure at 66 bytes for multi-relay multi-hop network.

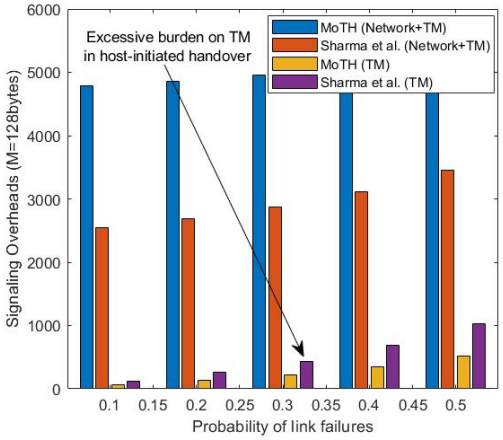

Fig. 6. Signaling overhead vs. probability of link failure at 128 bytes for multi-relay multi-hop network.

A. Multi-relay multi-hop network: IoT-enabled smart-city scenario

It is to be specifically considered that in multi-relay multi-hop setup network-based handover approaches have high signal consumption compared to the host-based approach (Sharma et al. [15]) as most of the signals are to be initiated by the network infrastructure. However, the major advantage is that the network-based approaches (MoTH) have a lower impact on the host and can provide better services at lower consumption of resources.

This is one of the advantages of using the proposed protocol for smart city applications where the number of end-users increases exponentially. In addition to this, with most of the approaches carried in the network, the entire handover process is independent of the type of the host, i.e., TM technologies and far more flexibility and better key updates along with reconfiguration can be obtained which otherwise are tedious to

attain with host-based approaches. Despite these key differences, we also provided the host-only impact along with the overall signaling overheads in the proposed approach in Fig. 5 and Fig. 6.

The overall cost may be higher but the signaling overheads for the TMs are lower, which shows that better performance can be obtained at lower consumption of resources. Moreover, with this, the security of the entire system is governed by the network infrastructure, offering a lower window to attackers that can compromise the TM. The probability of failure has a significant impact on the performance of the system. Here, a crucial point to be noted is with the increasing probability of failures, the overall signaling cost increases, however, from the host (TMs) point of view, the signaling overheads are lower in the proposed protocol as most of the impact of failure is covered by the signaling messages between the hubs and BMF.

Another parameter is the handover latency, which is proportional to the signaling overhead associated with the completion of the handoff. It is slightly higher in the case of MoTH, however, in terms of values, this is still limited and does not impact the overall performance of the system even with strong security requirements, as shown in Fig. 7. In the initial phase, the MoTH consumes 40 ms more time because of the inclusion of the long pass between the TM and BMF-ASF. However, this is overpowered by the security gains attained because of the involvement of the 5G security function as well as resource consumption of TM, which will considerably decrease as major of the operations are handled at the network level. The proposed approach reduces the burden on the TM by 50% for both signaling overhead and handover latency in comparison with Sharma et al. [15].

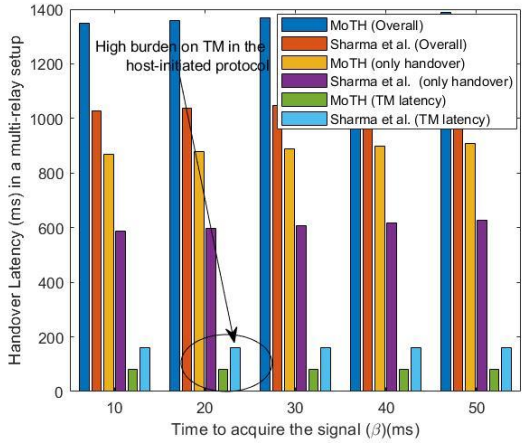

Fig. 7. Handover latency vs. time to acquire the signal for multi-relay multi-hop network.

B. Single-relay multi-hop network: IoT-enabled industrial scenario

Single-relay mode is the actual way of comparing protocols as it presents the details only relying on the messages which are shared between the entities. Even the delays in terms of handover latencies are the true representation of the message computational overheads, not the distance between the hops. We used the similar modeling as used in the multi-relay setup from Table VI and compared the protocol with Sharma et al. As shown in Fig. 8 and Fig. 9, the overall as well as the TM

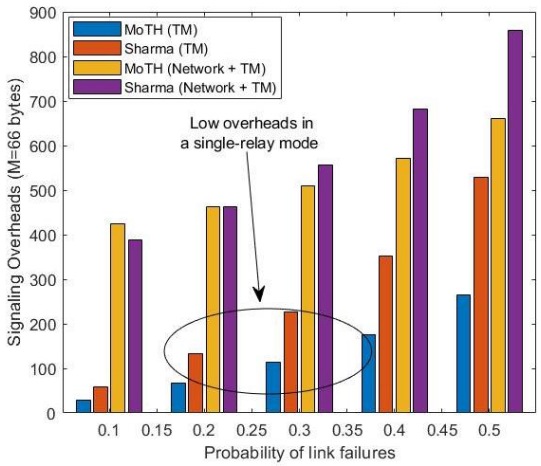

Fig. 8. Signaling overhead vs. probability of link failure at 66 bytes for single-relay multi-hop network.

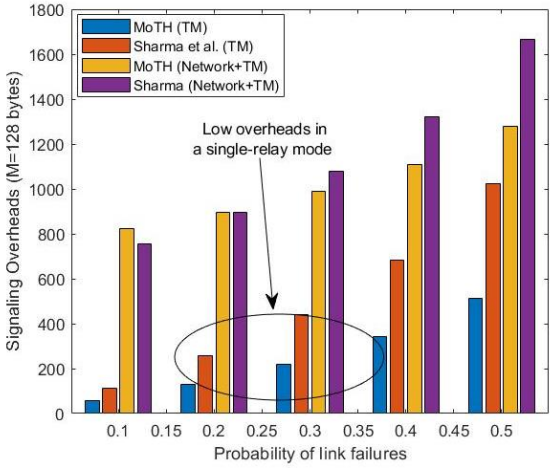

Fig. 9. Signaling overhead vs. probability of link failure at 128 bytes for single-relay multi-hop network.

signaling overheads are lower for different message sizes as it only considers a single-relay network where the TM operates in the direct periphery of the hubs and the hubs are only two-hop distance from the ASF.

Alongside this, Fig. 10 shows the impact of the signaling overheads on the handover latency in the single-relay mode. As host-based protocols [15], which are driven by the maximum signals at the TM and the proposed protocol has maximum operation at the network, the decrease in the number of relays improves the performance of the proposed protocol by 16.6%. It can be observed that TM latency is unaffected irrespective of the mode of operation and it remains high for the host-initiated protocols.

Irrespective of the multi-relay or single-relay system (any application), Fig. 11 helps to understand the reliability of the handover at the TM end when it is moving across the network. The results show that as most of the signals in the MoTH are carried between the network entities, its reliability is higher than the protocol proposed in Sharma et al. [15].

Generally, once the initial phase is executed, the key update phase is called after the key lifetime is expired. The frequency of this phase is decided based on the security level. Here is a trade-off between security and efficiency. That is, the more frequently the key update phase is called, the stronger the security becomes. In this case, the key update overhead

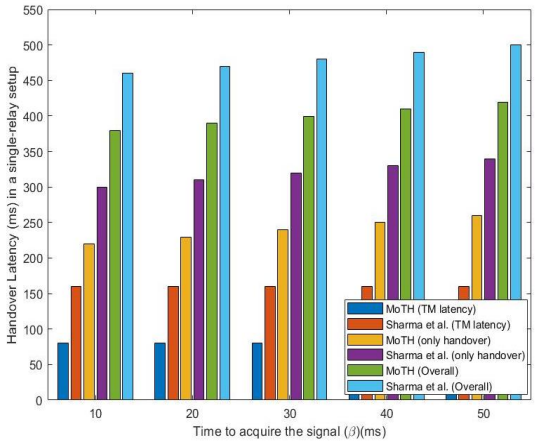

Fig. 10. Handover latency vs. time to acquire the signal for single-relay multi-hop network.

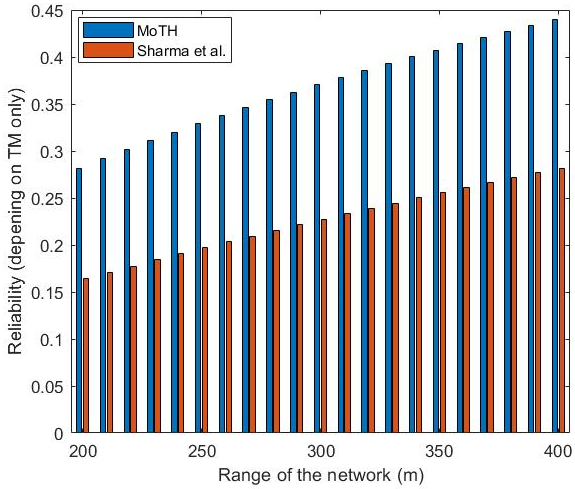

Fig. 11. TM's reliability vs. range of the network (coverage).

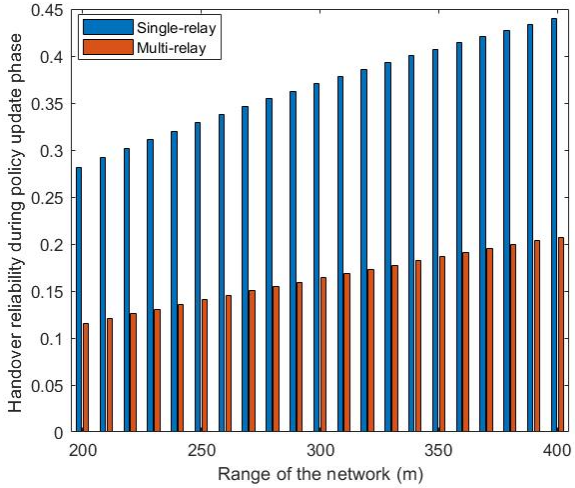

Fig. 12. Handover reliability during policy update phase vs. range of the network (coverage).

increases while sacrificing efficiency. In the opposite case, the key update overhead decreases while sacrificing security. Irrespective of this, the protocol offers updates at comparable rates. Specifically, the security reliability of the update phase can help to understand how much the impact of the additional overheads are caused on the overall operations, as shown in Fig. 12, assuming that the line of sight is available during the update phase, and there is no additional latency associated with it. It is evident from the figure that with updates, an overhead of 80 and 240 ms are added for single-relay and multi-relay, respectively. However, this provides a reliability of 0.26 and 0.11, respectively, in the policy update phase for a fast-moving TM, which otherwise would require re-initialization. Here, the trade-off can be understood by skipping the additional security mechanism of the update phase, which can enhance the reliability of handover up to 0.4 of the range of the network is up to 400 m. It is to be noted that the existing protocols even for fronthaul security are not considering the policy update phase and lack their position on flexible and adaptive security.

Thus, it can be expressed that with a network-based mechanism, MoTH offers reliable handover with better security features for backhaul networks at a comparable handover latency and signaling overheads that can be considered as an essential solution for providing backhaul handover security for smart city applications and their industrial setup.

VI. Conclusion

Flexible and adaptive handover management can enhance the security of 5GB-enabled IoT networks. With the inclusion of mobile terminals across the Hub-switch architecture as a backhaul, the security becomes tedious to attain as factors like perfect forward secrecy, non-compromising entities become important to attain. The resolution of these issues helps to obtain an efficient and secure network with better coverage as mobile terminals can be used for providing services in non-reachable areas. This paper considered mobility management across the backhaul and proposed a protocol, MoTH, which uses the basics of P2MP-backhaul security protocol. The proposed protocol is adaptive and periodic key updates to ensure the security of the parties involved in the handover. The protocol can protect information and secure exchange messages between the terminals that move across the hubs. The use of 5G security functions helps to derive a backhaul mobility function which regulates the handover procedures. The proposed protocol can serve as the basis for further development as most of the existing works are focused on fronthaul mobility management, and the ones which focus on backhaul security do not cover the handovers. The security of the proposed protocol is demonstrated by using the BAN logic and its correctness is derived using Scyther tool.

Furthermore, the protocol is compared with some of the existing security protocols, which predominately operate for device authentication and authorization. The proposed protocol provides secure handover in a backhaul environment at comparable computational overheads. Alongside this, a numerical case study showed the impact of the protocol in a multi-relay multi-hop and single-relay multi-hop network in terms of signaling overheads and handover latency. The proposed protocol improves the issues associated with the dependencies on the host as it is a network initiated and such facilitation lowers the burden on the terminals, thus, improving the overall reliability of the network. However, currently, the multi-relay multi-hop network shows some additional overheads, although negligible, these can be improved by appropriately designing the security functions and selecting

their placement in the network to reduce the number of passes. Such tasks are not dealt with in the current version and left to the future works.

APPENDIX AND SUPPLEMENTARY FILES

The BAN logic equations are provided at the end of the paper as Appendix, and the codes for Scyther are provided as separate files.

REFERENCES

[1] Takehiro Nakamura,. 2020. “5G Evolution and 6G.” In *2020 IEEE Symposium on VLSI Technology*, 1–5.

[2] Union, I. 2015. “IMT Traffic Estimates for the Years 2020 to 2030.” *Report ITU*, 2370.

[3] Gaurav Choudhary, Jiyoon Kim, and Vishal Sharma. "Security of 5G-Mobile Backhaul Networks: A Survey." Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 9(4) (2018): 41-70.

[4] Mostafa Zaman Chowdhury, Md Shahjalal, Shakil Ahmed, and Yeong Min Jang. 2020. “6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions.” *IEEE Open Journal of the Communications Society* 1 (July): 957–75.

[5] Latif U Khan, Ibrar Yaqoob, Muhammad Imran, Zhu Han, and Choong Seon Hong. 2020. “6G Wireless Systems: A Vision, Architectural Elements, and Future Directions.” *IEEE Access* 8: 147029–44.

[6] Jiyoon Kim, Gaurav Choudhary, Jaejun Heo, Daniel Gerbi Duguma, and Ilsun You. "5G wireless P2MP backhaul security protocol: an adaptive approach." *EURASIP Journal on Wireless Communications and Networking* 2019, no. 1 (2019): 265.

[7] Sabrina Sicari, Alessandra Rizzardi, and Alberto Coen-Porisini. "5G on the Internet of Things era: an overview on security and privacy challenges." Computer Networks (2020): 107345.

[8] Sooeun Song, Minsu Choi, Yunyeong Goh, Jusik Yun, Wonsuk Yoo, Wonsik Yang, Jaewook Jung, and Jong Moon Chung. 2020. “Analysis of Wireless Backhaul Networks Based on Aerial Platform Technology for 6g Systems.” *Computers, Materials and Continua* 62 (2): 473–94.

[9] Mohammed H lsharif, Anabi Hilary Kelechi, Mahmoud A Albreem, Shehzad Ashraf Chaudhry, M Sultan Zia, and Sunghwan Kim. 2020. “Sixth Generation (6G) Wireless Networks: Vision, Research Activities, Challenges and Potential Solutions.” *Symmetry* 12 (4): 676.

[10] Michele Polese, Marco Giordani, Tommaso Zugno, Arnab Roy, Sanjay Goyal, Douglas Castor, and Michele Zorzi. "Integrated Access and Backhaul in 5G mmWave Networks: Potential and Challenges." IEEE Communications Magazine 58, no. 3 (2020): 62-68.

[11] Jiaqi Huang and Yi Qian. "A Secure and Efficient Handover Authentication and Key Management Protocol for 5G Networks." Journal of Communications and Information Networks 5, no. 1 (2020): 40-49.

[12] Kamal Ali Alezabi, Fazirulhisyam Hashim, Shaiful J. Hashim, Borhanuddin M. Ali, and Abbas Jamalipour. "Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks." EURASIP Journal on Wireless Communications and Networking 2020 (2020): 1-34.

[13] Jianbing Ni, Xiaodong Lin, and Xuemin Sherman Shen. "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT." IEEE Journal on Selected Areas in Communications 36, no. 3 (2018): 644-657.

[14] Ning Wang, Pu Wang, Amir Alipour-Fanid, Long Jiao, and Kai Zeng. "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities." IEEE Internet of Things Journal 6, no. 5 (2019): 8169-8181.

[15] Vishal Sharma, Ilsun You, Fang-Yie Leu, and Mohammed Atiquzzaman. "Secure and efficient protocol for fast handover in 5G mobile Xhaul networks." *Journal of Network and Computer Applications* 102 (2018): 38-57.

[16] Dan Simon, Bernard Aboba, and Ryan Hurst. "The EAP-TLS authentication protocol." *RFC 5216* (2008) [Last Accessed: June 2020].

[17] Jari Arkko and Henry Haverinen. Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA). RFC 4187, January 2006 [Last Accessed: June 2020].

[18] Hannes Tschofenig, Dirk Kroeselberg, Andreas Pashalidis, Yoshihiro Ohba, and Florent Bersani. "The extensible authentication protocol-Internet key exchange protocol version 2 (EAP-IKEv2) method." *RFC 5106 (Experimental)* (2008) [Last Accessed: June 2020].

[19] Pekka Nikander, Andrei Gurtov, and Thomas R. Henderson. "Host identity protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks." *IEEE Communications Surveys & Tutorials* 12, no. 2 (2010): 186-204.

[20] Madhusanka Liyanage, Mika Ylianttila, and Andrei Gurtov. "A case study on security issues in LTE backhaul and core networks." *Case Studies in Secure Computing: Achievements and Trends* 1 (2014): 167.

[21] Alexandros Kaloxylos, Panagiotis Spapis, and Ioannis Moscholios. "SDN-Based Session and Mobility Management in 5G Networks." *Wiley 5G Ref: The Essential 5G Reference Online* (2019): 1-17.

[22] Vishal Sharma, Jiyoon Kim, Yongho Ko, Ilsun You, and Jung Taek Seo. "An Optimal Security Management Framework for Backhaul-aware 5G-Vehicle to Everything (V2X)." *Journal of Internet Technology* 21, no. 1 (2020): 245-260.

[23] Rakibul Islam Rony, Akshay Jain, Elena Lopez-Aguilera, Eduard Garcia-Villegas, and Ilker Demirkol. "Joint access-backhaul perspective on mobility management in 5G networks." In *Conference on Standards for Communications and Networking (CSCN)*, pp. 115-120. IEEE, 2017.

[24] Shengdun Hu, Xianbin Wang, and Muhammad Zeeshan Shakir. "A MIH and SDN-based framework for network selection in 5G HetNet: Backhaul requirement perspectives." In *International conference on communication workshop (ICCW)*, pp. 37-43. IEEE, 2015.

[25] Jianfeng Guan, Vishal Sharma, Ilsun You, Mohammed Atiquzzaman, and Muhammad Imran. "Extension of MIH for FPMIPv6 (EMIH-FPMIPv6) to support optimized heterogeneous handover." *Future Generation Computer Systems* 97 (2019): 775-791.

[26] Vishal Sharma, Ilsun You, Francesco Palmieri, Dushantha Nalin K. Jayakody, and Jun Li. "Secure and energy-efficient handover in fog networks using blockchain-based DMM." *IEEE Communications Magazine* 56, no. 5 (2018): 22-31.

[27] Michael Burrows, Martin Abadi, and Roger Michael Needham. "A logic of authentication." Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 426, no. 1871 (1989): 233-271.

[28] Catherine A. Meadows, "Formal verification of cryptographic protocols: A survey." In International Conference on the Theory and Application of Cryptology, pp. 133-150. Springer, Berlin, Heidelberg, 1994.

[29] Cas JF. Cremers, "The Scyther Tool: Verification, falsification, and analysis of security protocols." In International conference on computer aided verification, pp. 414-418. Springer, Berlin, Heidelberg, 2008.

[30] Colin Boyd and Wenbo Mao. "On a limitation of BAN logic." In Workshop on the Theory and Application of Cryptographic Techniques, pp. 240-247. Springer, Berlin, Heidelberg, 1993.

[31] Cas JF. Cremers and S. Mauw. “Security Properties.” In Operational Semantics and Verification of Security Protocols (pp.37-63). Springer, Berlin, Heidelberg.

[32] Jong-Hyouk Lee and Jean-Marie Bonnin. "HOTA: Handover optimized ticket-based authentication in network-based mobility management." *Information Sciences* 230 (2013): 64-77.

[33] Janise McNair, Ian F. Akyildiz, and Michael D. Bender. "An inter-system handoff technique for the IMT-2000 system." In Proceedings Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No. 00CH37064), vol. 1, pp. 208-216. IEEE, 2000.

[34] Ilsun You and Jong-Hyouk Lee. "SPFP: Ticket-based secure handover for fast proxy mobile IPv6 in 5G networks." *Computer Networks* 129 (2017): 363-372.

JIYOON KIM (S’20) received the M.S. degree in information security engineering from Soonchunhyang University, South Korea, where he is currently pursuing the PhD degree in the Department of Information Security Engineering. His current research interests include mobile internet security, 5G security, and formal security analysis.

PHILIP VIRGIL ASTILLO received the B.S. degree in computer engineering from University of San Carlos, Cebu, Philippines in 2009 and the M.Eng. degree in computer engineering from the same university in 2011. He is currently pursuing the Ph.D. degree in Information Security Engineering at Soonchunhyang University, South Korea. From 2009 to 2015, he worked as a lecturer in the University of San Carlos. From 2014 to 2015, he was a Research Assistant with the Phil-LiDAR Program in the same university. From 2015 to 2016, he was a Research Assistant with Sensor Laboratory of Clemson University, South Carolina, USA. His research interests include sensor development, embedded system design and development, mobile Internet security, 5G security, and IoT security.

VISHAL SHARMA (S'13-M'17) received the PhD and BTech degrees in computer science and engineering from Thapar University (2016) and Punjab Technical University (2012), respectively. He is working as a Lecturer (~Assistant Professor) in the School of Electronics, Electrical Engineering and Computer Science (EEECS) at the Queen's University Belfast (QUB), Northern Ireland, United Kingdom. Before coming to QUB, he was a Research Fellow in the Information Systems Technology and Design (ISTD) Pillar at the Singapore University of Technology and Design (SUTD), Singapore where he worked on the future-proof blockchain systems funded by SUTD-MoE. From Nov'16 to Mar'19, he worked in the Information Security Engineering Department at Soonchunhyang University, South Korea in multiple positions (Nov'16 to Dec'17: Postdoctoral Researcher; Jan'18 to Mar'19: Research Assistant Professor). He also held a joint postdoctoral position with Soongsil University, South Korea. He was affiliated with the Industry-Academia Cooperation Foundation and the Mobile Internet Security lab at Soonchunhyang University. Before this, he worked as a lecturer in the Computer Science and Engineering Department at Thapar University, India. He is the recipient of three best paper awards from the International Conference on Communication, Management and Information Technology (ICCMIT), Warsaw, Poland, in April 2017; from CISC-S'17 South Korea in June 2017; and from IoTaas Taiwan in September 2017. He is the member of IEEE, a professional member of ACM and past Chair for ACM Student Chapter-TIET Patiala. He has authored/co-authored more than 100 journal/conference articles and book chapters and co-edited two books with Springer. He served/serving as a guest editor of MIS, IJDSN, WCMC, MDPI (Sensors, Drones, Future Internet), and Autosoft journals. He was the track chair of MobiSec'16 and AIMS-FSS'16, and PC member and reviewer of MIST'16 and MIST'17, respectively. He has served/serving as the TPC member of ETIC- 2019, WiMO-2019, ITNAC-IEEE TCBD'17, ICCMIT'18, CoCoNet'18, and ITNAC-IEEE TCBD'18. Furthermore, he serves as a reviewer for various ACM/IEEE Transactions and other journals. He also serves as the ATE for the IEEE Communications Magazine and an AE for the IET-CAAI TRIT, Wireless Communications and Mobile Computing, and IET Networks. His areas of research and interests are 5G networks, Blockchain systems, aerial (UAV) communications, CPS-IoT behavior-modeling, and mobile Internet systems.

NADRA GUIZANI is a Clinical Assistant Professor at Washington State University. Her research interests include machine learning, mobile networking, large data analysis, and prediction techniques. She is an active member of both the Women in Engineering program and the Computing Research Association.

ILSUN YOU (SM'13) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Japan, in 2012. He is currently working as an associate professor at the Department of Information Security Engineering, Soonchunhyang University, South Korea. His main research interests include Internet security, authentication, access control, and formal security analysis. He is the EiC of the Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), and Journal of Internet Services and Information Security (JISIS). He is on the Editorial Board of Information Sciences, Journal of Network and Computer Applications, International Journal of Ad Hoc and Ubiquitous Computing, Computing and Informatics, Intelligent Automation and Soft Computing, and so on. He is a Fellow of the IET.

APPENDIX A. FORMAL VERIFICATION WITH BAN LOGIC (INIT PHASE)

$(I1)\ TM \rightarrow ASF: \langle ID_{TM}, ID_{ASF}, ts, n_1, capability \rangle_{K_{TM,ASF}}$
$(I2)\ HUB \rightarrow TM: \langle ID_{HUB}, ID_{TM}, n_1, n_2, g^Y, policy, TM \overset{MK}{\Leftrightarrow} HUB \rangle_{MK}$
$(I3)\ TM \rightarrow HUB: \langle ID_{TM}, ID_{HUB}, n_2, g^X, TM \overset{MK}{\Leftrightarrow} HUB \rangle_{MK}, \langle TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB \rangle_{AK}$
$(I4) HUB \rightarrow TM: \langle ID_{HUB}, ID_{TM}, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB \rangle_{AK}$

EQUATION 1. Idealizations (Init Phase)

$(AI1)\ ASF\ believes\ TM \overset{K_{TM,ASF}}{\Longleftrightarrow} ASF$
$(AI2)\ ASF\ believes\ \#(ts)$
$(AI3)\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(AI4)\ TM\ believes\ \#(n_1)$
$(AI5)\ TM\ believes\ \overset{g^X}{\rightarrow} TM$
$(AI6)\ HUB\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(AI7)\ HUB\ believes\ \#(n_2)$
$(AI8)\ HUB\ believes\ \overset{g^Y}{\rightarrow} HUB$
$(AI9)\ HUB\ believes\ \#\left(TM \overset{AK}{\Leftrightarrow} HUB\right)$
$(AI10)\ TM\ believes\ \#\left(TM \overset{AK}{\Leftrightarrow} HUB\right)$

EQUATION 2. Assumptions (Init Phase)

$(GI1)\ ASF\ believes\ TM\ believes\ ID_{TM}$
$(GI2)\ TM\ believes\ HUB\ believes\ ID_{HUB}$
$(GI3)\ TM\ believes\ HUB\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(GI4)\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} HUB$
$(GI5)\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} HUB$
$(GI6)\ HUB\ believes\ TM\ believes\ ID_{TM}$
$(GI7)\ HUB\ believes\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(GI8)\ HUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB$
$(GI9)\ HUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB$
$(GI10)\ HUB\ believes\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} HUB$
$(GI11)\ HUB\ believes\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} HUB$
$(GI12)\ TM\ believes\ HUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB$
$(GI13)\ TM\ believes\ HUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB$

EQUATION 3. Goals (Init Phase)

From (I1), we derive:
$(D1)\ ASF\ sees\ \langle ID_{TM}, ID_{ASF}, ts, n_1, capability \rangle_{K_{TM,ASF}}$
$(D2)\ ASF\ believes\ TM\ said\ (ID_{TM}, ID_{ASF}, ts, n_1, capability)\ by\ (D1), (AI1), MM$
$(D3)\ ASF\ believes\ TM\ believes\ (ID_{TM}, ID_{ASF}, ts, n_1, capability)\ by\ (D2), (AI2), FR, NV, BC$
$(D4)\ ASF\ believes\ TM\ believes\ ID_{TM}\ \ by\ (D3), BC$

From (I2), we derive:
$(D5)\ TM\ sees\ \langle ID_{HUB}, ID_{TM}, n_1, n_2, g^Y, policy, TM \overset{MK}{\Leftrightarrow} HUB \rangle_{MK}$
$(D6)\ TM\ believes\ HUB\ said\ \left(ID_{HUB}, ID_{TM}, n_1, n_2, g^Y, policy, TM \overset{MK}{\Leftrightarrow} HUB\right)\ by\ (D5), (AI3), MM$
$(D7)\ TM\ believes\ HUB\ believes\ \left(ID_{HUB}, ID_{TM}, n_1, n_2, g^Y, policy, TM \overset{MK}{\Leftrightarrow} HUB\right)\ by\ (D6), (AI4), FR, NV$
$(D8)\ TM\ believes\ HUB\ believes\ ID_{HUB}\ \ by\ (D7), BC$
$(D9)\ TM\ believes\ HUB\ believes\ TM \overset{MK}{\Leftrightarrow} HUB\ \ by\ (D7), BC$
$(D10)\ TM\ believes\ TM \overset{g^{XY}}{\Leftrightarrow} HUB\ \ by\ (D6), BC, (AI5), DH$
$(D11)\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ \ by\ (D10), (AI3), (D7), BC$
$(D12)\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ \ by\ (D10), (AI3), (D7), BC$

From (I3), we derive:
$(D13)\ HUB\ sees\ \langle ID_{TM}, ID_{HUB}, n_2, g^X, TM \overset{MK}{\Leftrightarrow} HUB \rangle_{MK}, \langle TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB \rangle_{AK}$
$(D14)\ HUB\ believes\ TM\ said\ \left(ID_{TM}, ID_{HUB}, n_2, g^X, TM \overset{MK}{\Leftrightarrow} HUB\right)\ by\ (D13), (AI6), MM$
$(D15)\ HUB\ believes\ TM\ believes\ \left(ID_{TM}, ID_{HUB}, n_2, g^X, TM \overset{MK}{\Leftrightarrow} HUB\right)\ by\ (D14), (AI7), FR, NV$
$(D16)\ HUB\ believes\ TM\ believes\ ID_{TM}\ \ by\ (D15), BC$
$(D17)\ HUB\ believes\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} HUB\ by\ (D15), BC$
$(D18)\ HUB\ believes\ TM \overset{g^{XY}}{\Leftrightarrow} HUB\ \ by\ (D14), BC, (AI8), DH$
$(D19)\ HUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ by\ (D18), (AI6), (D14), BC$
$(D20)\ HUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ by\ (D18), (AI6), (D14), BC$
$(D21)\ HUB\ believes\ TM\ said\ \left(TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\right)\ by\ (D13), (D19), MM$
$(D22)\ HUB\ believes\ TM\ believes\ \left(TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\right)\ by\ (D21), (AI9), FR, NV$
$(D23)\ HUB\ believes\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ by\ (D22), BC$
$(D24)\ HUB\ believes\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ by\ (D22), BC$

From (I4), we derive:
$(D25)\ TM\ sees\ \langle ID_{HUB}, ID_{TM}, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB \rangle_{AK}$
$(D26)\ TM\ believes\ HUB\ said\ \left(ID_{HUB}, ID_{TM}, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\right)\ by\ (D25), (D11), MM$
$(D27)\ TM\ believes\ HUB\ believes\ \left(ID_{HUB}, ID_{TM}, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\right)\ by\ (D26), (AI10), FR, NV$
$(D28)\ TM\ believes\ HUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ by\ (D27), BC$
$(D29)\ TM\ believes\ HUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ by\ (D27), BC$

APPENDIX B. FORMAL VERIFICATION WITH BAN LOGIC (POLICY UPDATE PHASE)

$(I5)\ HUB \rightarrow TM$: $\langle ID_{HUB}, ID_{TM}, ts, n_1, policy, g^Y, TM \overset{MK}{\Leftrightarrow} HUB\rangle_{MK}$
$(I6)\ TM \rightarrow HUB$: $\langle ID_{TM}, ID_{HUB}, n_1, n_2, g^X, TM \overset{MK}{\Leftrightarrow} HUB\rangle_{MK}, \langle TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\rangle_{AK}$
$(I7)\ HUB \rightarrow TM$: $\langle ID_{HUB}, ID_{TM}, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\rangle_{AK}$

EQUATION 4. Idealizations (Policy Update Phase)

$(AP1)\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(AP2)\ TM\ believes\ \#(ts)$
$(AP3)\ TM\ believes\ \overset{g^X}{\rightarrow} TM$
$(AP4)\ HUB\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(AP5)\ HUB\ believes\ \#(n_1)$
$(AP6)\ HUB\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(AP7)\ HUB\ believes\ \overset{g^Y}{\rightarrow} HUB$
$(AP8)\ TM\ believes\ \#(n_2)$

EQUATION 5. Assumptions (Policy Update Phase)

$(GP1)\ TM\ believes\ HUB\ believes\ policy$
$(GP2)\ TM\ believes\ HUB\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(GP3)\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} HUB$
$(GP4)\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} HUB$
$(GP5)\ HUB\ believes\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} HUB$
$(GP6)\ HUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB$
$(GP7)\ HUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB$
$(GP8)\ HUB\ believes\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} HUB$
$(GP9)\ HUB\ believes\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} HUB$
$(GP10)\ TM\ believes\ HUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB$
$(GP11)\ TM\ believes\ HUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB$

EQUATION 6. Goals (Policy Update Phase)

From (I5), we derive:

$(D28)\ TM\ sees\ \langle ID_{HUB}, ID_{TM}, ts, n_1, policy, g^Y, TM \overset{MK}{\Leftrightarrow} HUB\rangle_{MK}$
$(D29)\ TM\ believes\ HUB\ said$
$\left(ID_{HUB}, ID_{TM}, ts, n_1, policy, g^Y, TM \overset{MK}{\Leftrightarrow} HUB\right)\ by\ (D28), (AP1), MM$
$(D30)\ TM\ believes\ HUB\ believes$
$\left(ID_{HUB}, ID_{TM}, ts, n_1, policy, g^Y, TM \overset{MK}{\Leftrightarrow} HUB\right)\ by\ (D29), (AP2), FR, NV$
$(D31)\ TM\ believes\ HUB\ believes\ policy\ \ by\ (D30), BC$
$(D32)\ TM\ believes\ HUB\ believes\ TM \overset{MK}{\Leftrightarrow} HUB\ \ by\ (D30), BC$
$(D33)\ TM\ believes\ TM \overset{g^{XY}}{\Leftrightarrow} HUB\ \ by\ (D30), BC, (AP3), DH$
$(D34)\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ by\ (D33), (AP1), (D30), BC$
$(D35)\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ by\ (D33), (AP1), (D30), BC$

From (I6), we derive:

$(D36)\ HUB\ sees\ \langle ID_{TM}, ID_{HUB}, n_1, n_2, g^X, TM \overset{MK}{\Leftrightarrow} HUB\rangle_{MK}, \langle n_1, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\rangle_{AK}$
$(D37)\ HUB\ believes\ TM\ said\ \left(ID_{TM}, ID_{HUB}, n_1, n_2, g^X, TM \overset{MK}{\Leftrightarrow} HUB\right)\ by\ (D36), (AP4), MM$
$(D38)\ HUB\ believes\ TM\ believes$
$\left(ID_{TM}, ID_{HUB}, n_1, n_2, g^X, TM \overset{MK}{\Leftrightarrow} HUB\right)\ by\ (D37), (AP5), FR, NV$
$(D39)\ HUB\ believes\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} HUB\ by\ (D38), BC$
$(D40)\ HUB\ believes\ TM \overset{g^{XY}}{\Leftrightarrow} HUB\ by\ (D37), BC, (AP6), DH$
$(D41)\ HUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ by\ (D40), (AP4), (D37), BC$
$(D42)\ HUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ by\ (D40), (AP4), (D37), BC$
$(D43)\ HUB\ believes\ TM\ said\ \left(n_1, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\right)\ by\ (D36), (D40), MM$
$(D44)\ HUB\ believes\ TM\ believes\ \left(n_1, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\right)\ by\ (D43), (AP5), FR, NV$
$(D45)\ HUB\ believes\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ by\ (D44), BC$
$(D46)\ HUB\ believes\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ by\ (D44), BC$

From (I7), we derive:

$(D47)\ TM\ sees\ \langle ID_{HUB}, ID_{TM}, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\rangle_{AK}$
$(D48)\ TM\ believes\ HUB\ said$
$\left(ID_{TM}, ID_{HUB}, n_2, g^X, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\right)\ by\ (D47), (D34), MM$
$(D49)\ TM\ believes\ HUB\ believes$
$\left(ID_{TM}, ID_{HUB}, n_2, g^X, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} HUB\right)\ by\ (D48), (AP7), FR, NV$
$(D50)\ TM\ believes\ HUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ by\ (D49), BC$
$(D51)\ TM\ believes\ HUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ by\ (D49), BC$

APPENDIX C. FORMAL VERIFICATION WITH BAN LOGIC (HANDOVER PHASE)

$(I8)\ pHUB \rightarrow TM: \langle ID_{pHUB}, ID_{TM}, ts, policy\rangle_{MKold}$
$(I9)\ TM \rightarrow nHUB: \langle ID_{TM}, ID_{nHUB}, n_1, g^X, TM \overset{MK}{\Leftrightarrow} nHUB\rangle_{MK}$
$(I10)\ nHUB \rightarrow TM:$
$$\langle ID_{nHUB}, ID_{TM}, n_1, n_2, g^Y, TM \overset{MK}{\Leftrightarrow} nHUB\rangle_{MK}, \langle n_1, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} nHUB\rangle_{AK}$$
$(I11)\ TM \rightarrow nHUB: \langle ID_{TM}, ID_{nHUB}, n_2, TM \overset{AK}{\Leftrightarrow} nHUB, TM \overset{CK}{\Leftrightarrow} nHUB\rangle_{AK}$

EQUATION 7. Idealizations (Handover Phase)

$(AH1)\ TM\ believes\ TM \overset{MKold}{\Longleftrightarrow} pHUB$
$(AH2)\ TM\ believes\ \#(ts)$
$(AH3)\ nHUB\ believes\ TM \overset{MK}{\Leftrightarrow} nHUB$
$(AH4)\ nHUB\ believes\ \#\left(TM \overset{MK}{\Leftrightarrow} nHUB\right)$
$(AH5)\ nHUB\ believes\ \overset{g^Y}{\rightarrow} nHUB$
$(AH6)\ nHUB\ believes\ \#(n_2)$
$(AH7)\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} nHUB$
$(AH8)\ TM\ believes\ \#(n_1)$
$(AH9)\ TM\ believes\ \overset{g^X}{\rightarrow} TM$

EQUATION 8. Assumptions (Handover Phase)

$(GH1)\ TM\ believes\ pHUB\ believes\ policy$
$(GH2)\ nHUB\ believes\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} nHUB$
$(GH3)\ nHUB\ believes\ TM \overset{AK}{\Leftrightarrow} nHUB$
$(GH4)\ nHUB\ believes\ TM \overset{CK}{\Leftrightarrow} nHUB$
$(GH5)\ TM\ believes\ nHUB\ believes\ TM \overset{MK}{\Leftrightarrow} nHUB$
$(GH6)\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} nHUB$
$(GH7)\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} nHUB$
$(GH8)\ TM\ believes\ nHUB\ believes\ TM \overset{AK}{\Leftrightarrow} nHUB$
$(GH9)\ TM\ believes\ nHUB\ believes\ TM \overset{CK}{\Leftrightarrow} nHUB$
$(GH10)\ nHUB\ believes\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} nHUB$
$(GH11)\ nHUB\ believes\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} nHUB$

EQUATION 9. Goals (Handover Phase)

From (I8), we derive:
$(D52)\ TM\ sees\ \langle ID_{pHUB}, ID_{TM}, ts, policy\rangle_{MKold}$
$(D53)\ TM\ believes\ pHUB\ said\ \left(ID_{pHUB}, ID_{TM}, ts, policy\right)\ by\ (D52), (AH1), MM$
$(D54)\ TM\ believes\ pHUB\ believes\ \left(ID_{pHUB}, ID_{TM}, ts, policy\right)\ by\ (D53), (AH2), FR, NV$
$(D55)\ TM\ believes\ pHUB\ believes\ policy\ by\ (D54), BC$

From (I9), we derive:
$(D56)\ nHUB\ sees\ \langle ID_{TM}, ID_{nHUB}, n_1, g^X, TM \overset{MK}{\Leftrightarrow} nHUB\rangle_{MK}$
$(D57)\ nHUB\ believes\ TM\ said\ \left(ID_{TM}, ID_{nHUB}, n_1, g^X, TM \overset{MK}{\Leftrightarrow} nHUB\right)\ by\ (D56), (AH3), MM$
$(D58)\ nHUB\ believes\ TM\ believes$
$$\left(ID_{TM}, ID_{nHUB}, n_1, g^X, TM \overset{MK}{\Leftrightarrow} nHUB\right)\ by\ (D57), (AH4), FR, NV$$
$(D59)\ nHUB\ believes\ TM\ believes\ TM \overset{MK}{\Leftrightarrow} nHUB\ by\ (D58), BC$
$(D60)\ nHUB\ believes\ TM \overset{g^{XY}}{\Leftrightarrow} nHUB\ by\ (D57), BC, (AH5), DH$
$(D61)\ nHUB\ believes\ TM \overset{AK}{\Leftrightarrow} nHUB\ by\ (D60), (AH3), (AH6), BC$
$(D62)\ nHUB\ believes\ TM \overset{CK}{\Leftrightarrow} nHUB\ by\ (D60), (AH3), (AH6), BC$

From (I10), we derive:
$(D63)\ TM\ sees\ \langle ID_{nHUB}, ID_{TM}, n_1, n_2, g^Y, TM \overset{MK}{\Leftrightarrow} nHUB\rangle_{MK}, \langle n_1, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} nHUB\rangle_{AK}$
$(D64)\ TM\ believes\ nHUB\ said$
$$\left(ID_{nHUB}, ID_{TM}, n_1, n_2, g^Y, TM \overset{MK}{\Leftrightarrow} nHUB\right)\ by\ (D63), BC, (AH7), MM$$
$(D65)\ TM\ believes\ nHUB\ believes$
$$\left(ID_{nHUB}, ID_{TM}, n_1, n_2, g^Y, TM \overset{MK}{\Leftrightarrow} nHUB\right)\ by\ (D64), (AH8), FR, NV$$
$(D66)\ TM\ believes\ nHUB\ believes\ TM \overset{MK}{\Leftrightarrow} nHUB\ by\ (D65), BC$
$(D67)\ TM\ believes\ TM \overset{g^{XY}}{\Leftrightarrow} nHUB\ by\ (D64), BC, (AH9), DH$
$(D68)\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} nHUB\ by\ (D67), (AH7), (AH8), BC$
$(D69)\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} nHUB\ by\ (D67), (AH7), (AH8), BC$
$(D70)\ TM\ believes\ nHUB\ said\ \left(n_1, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} nHUB\right)\ by\ (D63), (D68), MM$
$(D71)\ TM\ believes\ nHUB\ believes$
$$\left(n_1, n_2, TM \overset{AK}{\Leftrightarrow} HUB, TM \overset{CK}{\Leftrightarrow} nHUB\right) by\ (D70), (AH8), FR, NV$$
$(D72)\ TM\ believes\ nHUB\ believes\ TM \overset{AK}{\Leftrightarrow} HUB\ by\ (D71), BC$
$(D73)\ TM\ believes\ nHUB\ believes\ TM \overset{CK}{\Leftrightarrow} HUB\ by\ (D71), BC$

From (I11), we derive:
$(D74)\ nHUB\ sees\ \langle ID_{TM}, ID_{nHUB}, n_2, TM \overset{AK}{\Leftrightarrow} nHUB, TM \overset{CK}{\Leftrightarrow} nHUB\rangle_{AK}$
$(D75)\ nHUB\ believes\ TM\ said$
$$\left(ID_{TM}, ID_{nHUB}, n_2, TM \overset{AK}{\Leftrightarrow} nHUB, TM \overset{CK}{\Leftrightarrow} nHUB\right)\ by\ (D74), (D60), MM$$
$(D76)\ nHUB\ believes\ TM\ believes$
$$\left(ID_{TM}, ID_{nHUB}, n_2, TM \overset{AK}{\Leftrightarrow} nHUB, TM \overset{CK}{\Leftrightarrow} nHUB\right)\ by\ (D75), (AH6), FR, NV$$
$(D77)\ nHUB\ believes\ TM\ believes\ TM \overset{AK}{\Leftrightarrow} nHUB\ by\ (D76), BC$
$(D78)\ nHUB\ believes\ TM\ believes\ TM \overset{CK}{\Leftrightarrow} nHUB\ by\ (D76), BC$