International Journal of Digital Information and Wireless Communications (IJDIWC) 4(4): 458-473
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2225-658X)

Analytical Approach of Cost-Effective and Secure SIP-based Mobility Management Scheme for NEMO Environments

Chulhee Cho[1], Jae-Young Choi[1], Jun-Dong Cho[2], and Jongpil Jeong[2,*]
[1]College of Information and Communication Engineering
Sungkyunkwan University, Suwon, Korea
[2]Department of Human ICT Convergence (*Corresponding Author)
Sungkyunkwan University, Suwon, Korea
tgb017@nate.com, {jaeychoi,jdcho,jpjeong}@skku.edu

ABSTRACT

The mobile Virtual Private Network (MVPN) of the Internet Engineering Task Force (IETF) is not designed to support NEtwork MObility (NEMO) and is not suitable for real-time applications. Therefore, architecture and protocols to support VPN in NEMO are needed. In this paper, we propose a cost-effective and secure mobility management scheme (SeSIP) that is based on session initiation protocol (SIP) and designed for real-time applications with VPN. Our scheme to support MVPN in NEMO enables the session to be well maintained during movement of the entire network. Further, in order to reduce the authentication delay time in handoff operations, the signaling time which occurs to maintain the session is shortened through our proposed handoff scheme which adopts authentication using HMAC-based one-time password (HOTP). Our performance analysis results show our proposed scheme provides improvement in average handoff performance time relative to existing schemes.

KEYWORDS

NEMO, MVPN, SIP, HOTP, Mobility Management.

1 INTRODUCTION

As the coverage area of wireless LAN (WLAN) expands, the demand from users is growing for access to the Internet anytime and anywhere. To satisfy this requirement, technologies that enable access to the Internet on trains, busses, ships, and other modes of transportations have come into the limelight. One such technology is NEMO, an IP network mobility technology [1-3]. The acronyms used in this paper is listed in Table 1. NEMO enables Internet connection service to be provided from the mobile router (MR) with all the nodes inside the network not recognizing the mobility, a standardization that is making progress in IETF based on IPv6. NEMO provides mobility service through direct links to the Internet network without passing through other networks. Thus, it can be applied to telematics, Personal Area Networks (PAN), Ad-hoc networks, etc., as well as providing various means of mobility. The IETF NEMO working group has completed several RFCs to enable a network to move from one location to another location while still maintaining its local nodes ongoing sessions. For example, a NEMO VPN can be used in public safety, where wireless devices in a police patrol car can access to the criminal databases, driver license and vehicle registration databases, or other services in the dispatch center as the car travels between different subnets. Similar type of services can also be used in ambulance or mobile medical car, where various wireless devices or sensors are deployed inside the car.

Security has recently emerged as an important issue for the Internet, and virtual private network (VPN) was developed to ensure stability in user communications between the Internet and the intranet. VPN service in NEMO has wide-ranging applications, providing stable access to the intranet for mobile networks. For example, NEMO VPN enables access to the criminal, driver's license, and car registration databases from a police patrol car via the mobile device, thereby helping to increase public safety. However, a method for providing VPN service has yet to be identified in the NEMO working group of IETF.

Although IETF proposed a VPN architecture that supports mobility, this solution did not consider mobile equipment groups and is only applicable for a single node, and, furthermore, it is based on MIP, which is not suited for real-time applications. MVPN of IETF uses one IPSec [4] tunnels and two MIP tunnels. These three tunnels are major contributors to overhead during the real-time packet transfer. Thus, a new architecture and protocol are required to support the MVPN in safe NEMO. In addition, the complexity of the authentication procedure and multiple signaling messages that may occur in various nodes due to the movement of the mobile equipment group are also major contributors to overhead.

This paper proposes a Cost Effective and Secure Mobility Management Scheme (SeSIP) based on the SIP (Session Initiation Protocol) which is suitable for real-time application on MVPN and which shortens the signaling time. This design maintains the session continuously as the overall network moves. It integrates SIP-based MVPN and NEMO to provide efficient group mobility for high security and real-time services. Additionally, all SIP clients can directly communicate with each other, bypassing the mobile agent such as the Home Agent (HA) in MIP. Thus, the path is optimized. This is useful for real-time applications such as IP-based voice communications (VoIP) and video streaming, and it does not require an IPSec tunnel or MIP tunnel. Hence, a single NEMO VPN gateway can support an entire mobile network upon the address request of a mobile network that has changed its connection location address, resulting in considerable reduction of signaling overhead. Moreover, this approach reduces the signaling numbers since all CNs connection addresses are combined in a URL list and integrated in a single INVITE message for transfer. Further, this design adopts an authentication method based on HMAC-based One Time Password (HOTP) [5] to shorten the authentication time, a significant element of delay during hand-off, thereby improving the ongoing signaling time to maintain the session. Moreover, this approach integrates the generation signals of multiple nodes inside the mobile network to reduce signaling time.

Table 1. Parameters for Handoff Signalling Cost.

Acronym	Description
ALG	Application Level Gateway
AVP	Attribute Value Pair
CN	Correspondent Node
CoA	Care of Address
HA	Home Agent
HMAC	Hash-based Message Authentication Code
HOTP	HMAC based One Time Password
IKE	Internet Key Exchange
i-HA	Internal HA
i-MIP	Internal MIP
MAA	Multimedia-Auth-Answer
MAR	Multimedia-Auth-Request
MIDCOM	Middlebox Communication
MIKEY	Multimedia Internet Keying
MIP	Mobile IP
MN	Mobile Node
MR	Mobile Router
NEMO	Network Mobility
OTP	One Time Passwords
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SA	Security Association
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP-NVG	SIP NEMO VPN Gateway
SRTP	Secure Real-time Transport Protocol
TEK	Traffic Encryption Key
TGK	TEK Generation Key
UAA	User-Authorization-Answer
UAR	User-Authorization-Request
VPN	Virtual Private Network
VPN-TIA	VPN Tunnel Inner Address
X-HA	external HA
X-MIP	external MIP

This paper consists of the following sections: Section 2 examines the problems of architecture for MVPN proposed in the existing IETF, and it looks into the need for a SIP-based MVPN. Section 3 describes the proposed SIP-based mobility management scheme which is cost

effective and secure. Section 4 discusses the analytical model to evaluate the functioning of the proposed scheme. Section 5 describes the numerical results for the analysis presented in Section 4. Finally, conclusions are drawn in Section 6.

2 RELATED WORK

IETF has previously defined the architecture and protocol for MVPN [6]; it is shown in Fig. 1. Here, the internal HA (i-HA) and external HA (x-HA) are present in the intranet and Internet and the two HAs. A new care-of address (CoA) is first obtained from the dynamic host configuration protocol (DHCP) server or foreign agent (FA) when the MN moves out of the intranet. This CoA is registered in x-HA. Then, MN creates a VPN gateway and IPSec tunnel using its external home address (x-HoA). An IPSec tunnel is created by using internet key exchange (IKE) [7]. Fig. 1 shows the three tunnels (x-MIP, IPSec, and i-MIP).

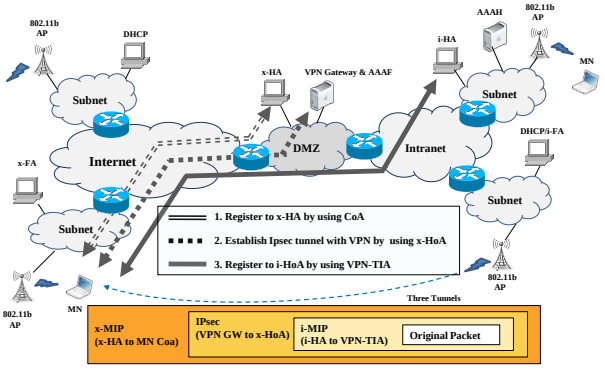

Figure 1. MVPN proposed by IETF.

Fig. 2 shows the signaling message flows of IETF MVPN. Because the mobility of a mobile equipment group was not considered in IETF MVPN, it cannot be applied to NEMO, since it would cause long handoff latency and end-to-end latency [8,9]. These tunnels significantly increase the overhead due to packet length and processing time, and this can degrade the performance in real-time applications. Although SIP-based MVPN was proposed, only the mobility of a single node was considered [10,11].

In this paper, we propose SIP-based NEMO because it is easily distributed and reduces the data transfer delay for host and session mobility [12,13]. However, if SIP is applied to NEMO, it may increase the handoff signaling cost, when many re-INVITE messages are transferred among the sessions in progress. HTTP digest is the basic user authentication realized in SIP. This authentication uses a secret key and is based on the challenge-response paradigm. Most protocols in Internet applications use this mechanism for client authentication before providing services; however, SIP authentication using HTTP digest increases the signaling exchange in the protocol design, requiring two handshakes to occur. To simplify the authentication procedure, we can instead adopt HOTP-based authentication, shortening processing time and so reducing signaling cost. Therefore, in this paper, we consider these methods for supporting the MVPN in NEMO and for shortening authentication time and signaling time in mobile networks, suitable for real-time applications.

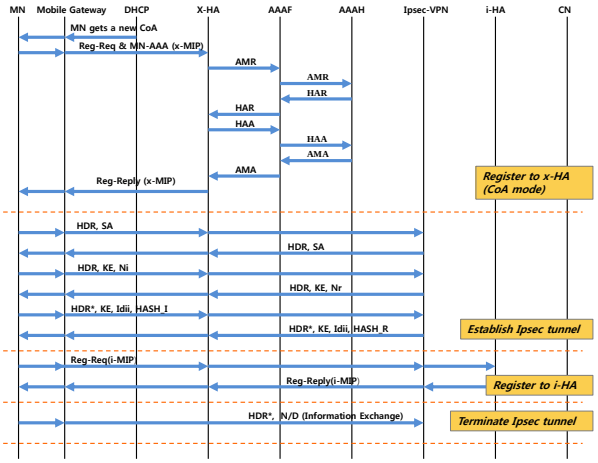

Figure 2. Signalling flows of IETF MVPN.

3 COST-EFFECTIVE AND SECURE MOBILITY MANAGEMENT SCHEME

3.1 System Architecture

IETF has defined architecture and protocols for mobile VPN. However, The IETF mobile VPN cannot be applied to NEMO because it does not consider the mobility of a group of mobile devices. Besides, the IETF solution is based on IPsec and MIPv4, so it will incur long handoff latency and

end-to-end latency. On the other hand, SIP has been proposed to provide host mobility and session continuity. However, by adopting SIP into NEMO, it may increase signaling cost during network handoff. So, I propose architecture and protocols to support VPN in NEMO, which is called Cost Effective and Secure Mobility Management Scheme [40]. The proposed SeSIP comprises SIP, secure real-time transport protocol (SRTP) [14], multimedia internet keying (MIKEY) [15], and a Diameter server [16] to provide VPN services in NEMO. Fig. 3 depicts the architecture of the proposed SeSIP.

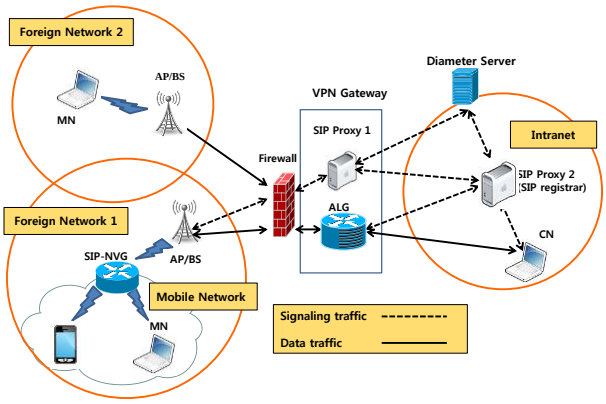

Figure 3. System architecture.

Fig. 3 shows a mobile network in a foreign network (Internet) connecting to the CN in the home network (intranet). The SIP NEMO VPN gateway (SIP-NVG) shown in the mobile network residing in Foreign Network 1 is the gateway of the mobile network to other networks. It follows the SIP standards and manages the traffic between the mobile network and the outside world. The VPN gateway consists of SIP Proxy 1 and an application level gateway (ALG). There is a firewall between the Internet and the intranet to prevent external users from getting direct access to the intranet. SIP Proxy 1 is a SIP proxy server, which authenticates the incoming SIP messages through the Diameter server. It also routes messages to SIP Proxy 2 which is essentially a SIP registrar. Meanwhile, MIKEY is used as the key management protocol to provide security keys for the ALG, which then oversees all data traffic.

In the proposed SeSIP, SIP is the main protocol to manage the session between MN, SIP-NVG, SIP Proxy 1, SIP Proxy 2, and CN. Diameter SIP Application [17] is an adaptation of the Diameter base protocol [16] that is used to authenticate and authorize a user in the Diameter server while resource allocation in ALG is achieved using Middle box Communication (MIDCOM) [18]. In addition, MIKEY messages are embedded inside the messages of the Diameter base protocol and the Session Description Protocol (SDP) [19] to carry security information. For user plane, when the mobile network resides in internet, SRTP is used to secure the data transmission between MN and ALG.

SIP is an application-layer signaling protocol. It is used to create, modify, and terminate sessions in the proposed SeSIP. SIP has defined its own security and authentication schemes. In our proposed CE-SeMMS, we use SIP to authenticate and identify the mobile users. SIP also supports user mobility and terminal mobility [12], [20]. Terminal mobility is achieved by sending new INVITE (re-INVITE) to the CN using the same call ID as that in the original session. The new INVITE contains the new contact address the MN has acquired in the new location. After receiving the re-INVITE, the CN will redirect future traffic to the MNs new location. SRTP defines a framework to provide encryption and integrity for Real-time Transport Protocol (RTP) [21] and RTP Control Protocol (RTCP) [21] streams.

MIKEY is a key management protocol developed for multimedia real-time applications running over RTP/SRTP. In contrast to IKE, which is widely used as key management protocol for unicast, MIKEY is designed for peer-to-peer or small interactive groups. MIKEY can fulfill the requirements of different environments. For example, a MIKEY message can be embedded inside an SDP message. A new type k has been defined in SDP to carry MIKEY message. The main purpose of MIKEY is to transport the TEK2 Generation Key(TGK) and other related security parameters or policies which are used in security transport protocols.

The Diameter SIP Application allows a client of a SIP server to be authenticated and authorized by a Diameter server. There are six Diameter commands in the Diameter SIP application. In the proposed SeSIP, we use User-Authorization-

Request (UAR) / User-Authorization-Answer (UAA) and Multimedia-Auth-Request (MAR) / Multimedia-Auth-Answer (MAA) to process SIP REGISTER and INVITE messages. The authentication is done by the Diameter server rather than by delegating to a SIP server. HOTP-based authentication is adopted in the proposed SeSIP to reduce authentication time, an element of delay time during handoff. HOTP is an OTP creation algorithm based on event synchronization, and the client and authentication server share the secret key K. It uses C, the increasing counter value, and HMAC-SHA-1 hash algorithm to create the password. The increased value (C +1) is used to create a new password (6 digits) during the following authentication. The OTP mechanism creates the single user password based on three parameters: hash algorithm, secret key, and challenge/counter. HOTP creates the password using the authentication number (counter) - which is remembered between the authentication server and the user - as the input value of OTP, and the authentication is performed only when the counter value matches. The counter parameter has the characteristics of synchronization OTP (HOTP [5]), and the client creates a new password without receiving the item beforehand from the authentication server. HOTP performs client authentication through one handshake, using the OTP creation algorithm based on the event synchronization method.

As discussed above, the SIP-NVG is the mobile networks gateway to other networks. When a mobile network roams among different IP subnets, the SIP-NVG not only keeps ongoing sessions unbroken, but also transmits data in a secure manner. There are two types of interfaces owned by SIP-NVG: egress interface and ingress interface. A SIP-NVG attaches to the Internet through an egress interface. Once a mobile network moves to a new IP subnet, the egress interface of the SIP-NVG will get a new IP address. On the other hand, when an MN wants to join a mobile network, it attaches to the ingress interface of the SIP-NVG. In our design, each mobile network has only one SIP-NVG which essentially is an MR with SIP capability. The proposed SIP-NVG is able to route SIP messages and data traffic between its egress interface and ingress interface by translating the corresponding headers.

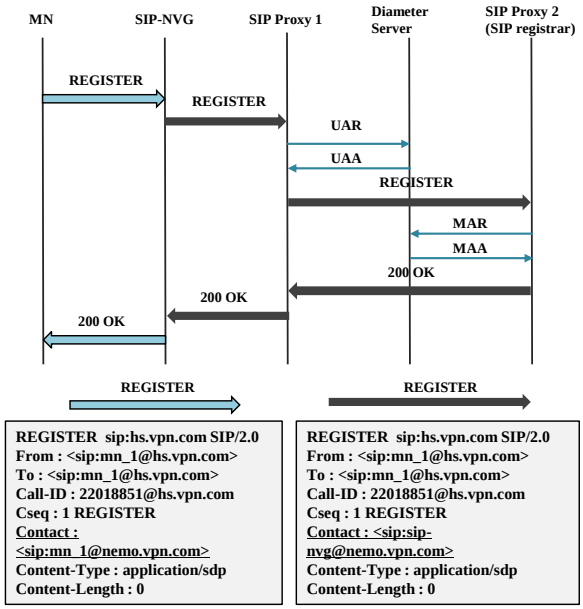

Figure 4. Message flows and translation of REGISTER when mobile network resides in foreign network.

Fig. 4 depicts the flow for registration when the mobile network is in a foreign network. When an MN enters a mobile network, the MN gets a new IP address and registers it with the SIP-NVG. As shown in Fig. 4, the MN updates its current location with the SIP registrar residing in the home network by sending the REGISTER with the newly obtained contact address. In this example, we assume the mobile network resides in a foreign network, and the new address assigned for the MN is mn-1@nemo.vpn.com. In our proposed architecture, SIP Proxy 2 not only handles the signaling messages but also acts as the SIP registrar. As illustrated in Fig. 4, the SIP-NVG translates the contact field in the REGISTER from the MNs address into the SIP-NVGs URI address, which is sip-nvg@hs.vpn.com. Also, the SIP-NVG establishes a mapping table to record the registration information for the MN. Hence, each request targeted to the MN is redirected to the SIP-NVG.

The proposed architecture depicted in Fig. 3 adopts an ALG which follows MIDCOM architecture. We propose that the ALG only accepts commands from SIP Proxy 2 and provides

responses for the corresponding commands. When the ALG receives a special incoming RTP stream from the home network to an MN in the Internet, it replaces the whole IP/UDP/RTP header with a new one, transforms the new RTP packet into SRTP format, and delivers the SRTP stream to the destination. In the reverse direction, the ALG receives the SRTP stream from the Internet, and the ALG decrypts it and verifies it to decide whether the SRTP packet is valid. If the SRTP packet is decrypted and verified successfully, the RTP payload is carried by a new RTP header. The new RTP packet is then transmitted to the home network.

Each session in the ALG requires sufficient external and internal resources. For example, the external resource may include an external listening address, external listening port, external destination address, and external destination port. Destination addresses and ports are provided by SIP Proxy 2. Only when all resources are ready, does the session in the ALG start. When either the external or internal resource is reserved successfully, the ALG will reply with the reserved listening address and port to SIP Proxy 2.

3.2 Operation Procedures

In the architecture shown in Fig. 3, the entire mobile network may move from one IP subnet to another. This is called network handoff. It is also possible that an MN moves into or moves out of the mobile network. This is called node handoff.

Fig. 5 depicts the flow when an MN moves into a mobile network which is located inside a foreign network. First, the MN registers with the SIP-NVG and the SIP registrar, as discussed in Section 3.2. Then, the MN must re-invite the CN, if there are active sessions between them. For the INVITE request, in addition to translating the CONTACT field from the MNs address into the SIP-NVGs URI address, the SIP-NVG also adds the RECORD-ROUTE field where the SIP-NVGs URI address is inserted. Therefore, subsequent messages of the existing sessions will be routed by the SIP-NVG. In this case, the signaling messages will need to go through SIP Proxy Server 1 and be authenticated by the Diameter Server before they reach SIP Proxy Server 2. When the mobile network and the CN are both located inside the same realm, for example, the same intranet or the same network domain in the Internet, the data traffic between the MNs attaching to the mobile network and the CN does not need to pass through the ALG. Instead, the data traffic is transmitted directly between the mobile network and CN. Thus, we assume that the CN is inside the intranet and that the mobile network moves between the intranet and the Internet. Using Fig. 3 as an example, we consider the cases when the mobile network moves from Home Network to Foreign Network 1, from Foreign Network 1 to Foreign Network 2, then from Foreign Network 2 back to the Home Network.

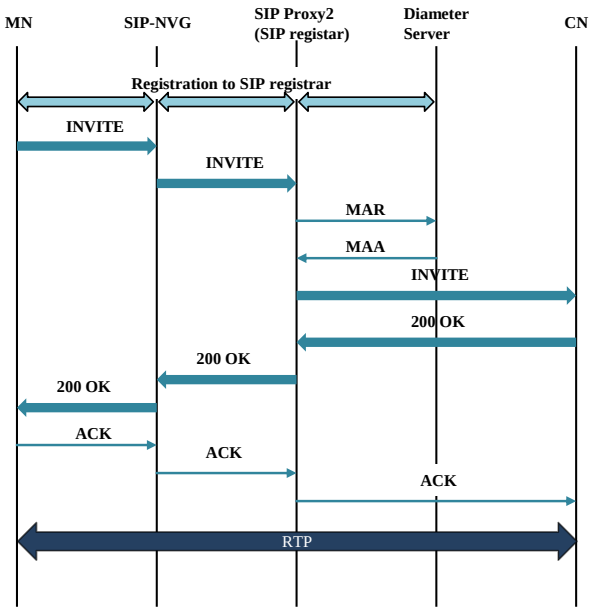

Figure 5. Message flows and translation of INVITE when MN moves to a mobile network which is located inside the home network.

Fig. 6 illustrates the flow when the mobile network moves from the intranet to the Internet. When a SIP-NVG moves to a foreign network, it must register with the SIP registrar using its new IP address. The SIP-NVG then checks whether there are MNs with active sessions inside the mobile network, according to the session table. The SIP-NVG must re-INVITE all CNs to recover all of the ongoing sessions. However, this process may cause substantial amounts of signaling

messages in the wireless links. In order to reduce the signaling overhead, the SIP-NVG combines all contact addresses of CNs into a URI list. The URI list is then conveyed by the SDP embedded in one INVITE message. The re-INVITE contains the new contact address of the SIP-NVG. This is sent to SIP Proxy 1, which routes the message to SIP Proxy 2, assuming that SIP Proxy 1 has been informed that SIP Proxy 2 is responsible for verification of ongoing sessions.

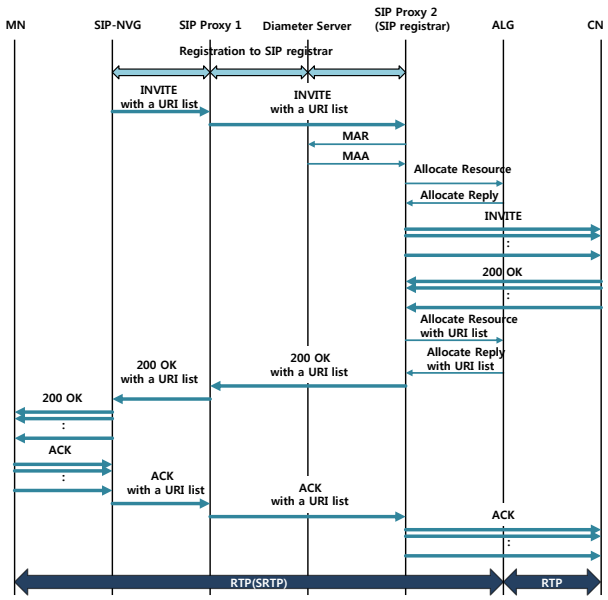

Figure 6. Message flows when mobile network roams from home network to foreign network.

SIP registrar, which received the INVITE message that includes the URI list, transmits each INVITE message to all CNs. CNs then transmit the response message (200 OK) to the SIP registrar if there are any active sessions. This process may also become a major contributor to the signaling message in the wireless link, and the SIP registrar, which received multiple response messages to reduce this signaling overhead, adds all connection addresses of CNs to the URI list and saves it. Later, the URI list is included in a single Allocate Resource command and transmitted to ALG. ALG then gives permission to the external resource through the URI list and then transmits the Allocate Reply response message to the SIP registrar. Then, SIP registrar transmits a response message, which includes the URI list in SDP, to SIP Proxy 1. The proposed SeSIP method adopts HOTP SIP authentication, for the authentication of each active session. HOTP performs client authentication through one handshake, using the OTP creation algorithm based on the event synchronization method. OTP is created based on the number of authentications which is the same as the time value synchronized between the client and the authentication server.

For HTTP digest authentication, a one-time password is created by using a certain random number as the input value of the password algorithm based on non-synchronization authentication. Therefore, if the authentication server creates a certain random number and transmits it to the user, the user creates the hash value using this random number. The user authentication is performed by responding to the resultant output value using the one-time password. This requires a handshake two times for authentication. Consequently, the signaling cost will increase. SIP-NVG saves the security information which is necessary for authentication, which shows MN when MN is connected to the mobile network. Fig. 7 shows an example of the password created with the HOTP algorithm [5] in the Call-ID of the SIP message header.

```
INVITE sip : mn_2@hs.vpn.com SIP/2.0
From : <sip : mn_1@hs.vpn.com>
To : <sip : mn_2@hs.vpn.com>
Call-ID : 238730@hs.vpn.com
Cseq : 43 INVITE
Content-Type : application/sip
Content-Length : 0
```

Figure 7. Example of a SIP Message including HOTP Call-Id

The Diameter command MAR/MAA in the Diameter SIP application is used to process authentication messages. To reduce the signaling overhead, the security information for each session is aggregated to one MAR/MAA message. This can be done easily by setting the reserved bit to M in the command flags within the MAR/MAAs Diameter header to indicate that there are multiple sessions to process. This causes SIP Proxy 2 to send the MAR to request the Diameter server to authenticate and authorize the sessions. Then, the diameter server compares the

password included in the Call-ID to the calculated password to determine authentication of the user agent. If the two values are the same, the Diameter server completes the user authentication through one handshake. The Diameter server informs SIP Proxy 2 of each sessions verification result, and it generates one pair of TGK and MIKEY for each verified session. Thereafter, the MAA has all the session verification result codes. To establish TGK and MIKEY message, pre-shared key, which is one of the most efficient ways to handle key transport, is used. The pairs of the TGK and MIKEY messages are transmitted to the SIP Proxy 2 by MAA.

If the SIP-NVG is granted access to the intranet, then SIP Proxy 2 must allocate enough resources to guarantee that the sessions will be protected. Thus, SIP Proxy 2 orders the ALG to reserve an internal receiving address and receiving port for each ongoing session. The command from SIP Proxy 2 may include the Data SA and the TGK for SRTP protection, and the CNs original listening addresses and listening ports. The ALG responds with the reserved addresses and ports. SIP Proxy 2 inserts the listening addresses and listening ports in the SDP to reproduce INVITE requests based on the URI list. It then routes them to each CN individually. Each CN sends back a 200 OK if it agrees with the SDP of the re-INVITE. After receiving the 200 OK from each CN, SIP Proxy 2 again orders the ALG to reserve the external receiving addresses and receiving ports. The ALG responds with the reserved external receiving addresses and receiving ports. If all allocated resources are ready, SIP Proxy 2 replaces the listening addresses and listening ports in the SDP of each 200 OK, and it inserts a MIKEY Initiator message into the SDP to transport the TGK. Then, SIP Proxy 2 sends each 200 OK with the new SDP to the SIP-NVG, which forwards it to the MN. The ALG will then start to function when both internal and external resources have been acquired. When each MN attaching to the mobile network receives the 200 OK, it must process the included MIKEY Initiator message and extract the shared TGK. The MN is then required to send an ACK with SDP which includes the MIKEY responder message. After the MN sends the ACK, it will start all transport sessions.

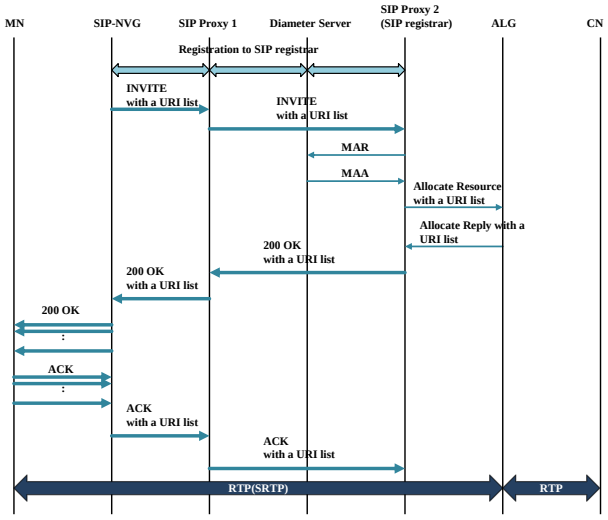

Figure 8. Message flow when the mobile network roams from one foreign network to another

Fig. 8 illustrates the flow when the mobile network moves again to another external network. The SIP-NVG must also update its new location with the Registrar and send re-INVITE to the CNs with active sessions. However, SIP Proxy 2 will function on behalf of the CNs to respond with the 200 OK. SIP Proxy 2 only orders the ALG to modify the external listening addresses and ports. The rest of the process is similar to that described for Fig. 6.

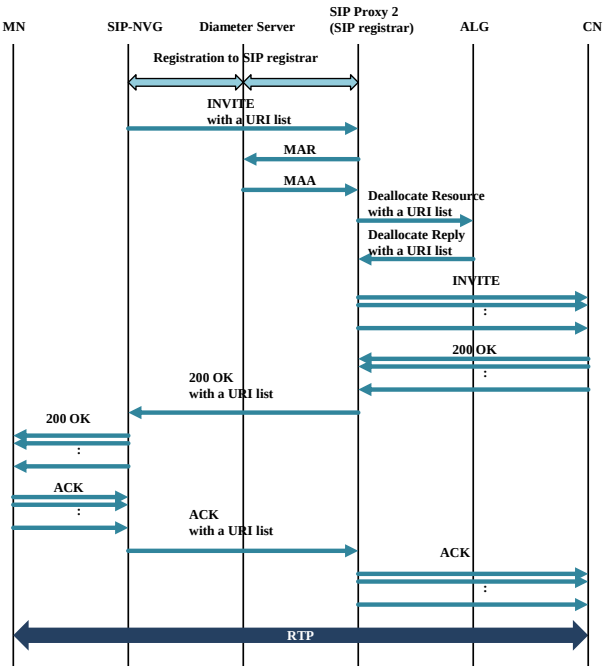

Figure 9. Message flow when the mobile network roams from a foreign network back to its home network

Fig. 9 depicts the flow when the mobile network moves back to the home network. Because the data traffic is secure within the intranet, the ALG is requested to deal locate both the internal and external resources. Because the proposed architecture is based on SIP rather than MIP, the problems of MIP, such as the overhead of three tunnels and potentially long end-to-end latency, are not problems in our design.

3.3 Security Vulnerabilities

SIP authentication: This section presents the qualitative analysis of security vulnerabilities in the proposed SeSIP. Integrity and confidentiality of SIP authentication messages are not protected. Therefore, malicious users may sniff traffic to get the plaintext or place a spam call. However, in the proposed SeSIP, the transport of SIP messages can be easily extended to incorporate Transport Layer Security (TLS) [22] so the transmission of SIP messages can be protected.

SIP parser attack: The free text format of SIP message could make parsing difficult. Attackers sending a very large messages with unnecessary headers and bodies can exhaust the resource of SIP server. The SeSIP may suffer from such attack too. To solve this problem, the parser in the SeSIP can be designed to check message size and discard the one which exceeds the size limit. Also, a practical implementation provided by [23], [24], [25] can be adopted.

4 PERFORMANCE ANALYSYS

4.1 System Modeling

In order to support secure communication in VPN, the proposed SeSIP sends signaling messages carrying security information. It also sends signaling messages to maintain session continuity during handoff. To evaluate the performance of the proposed SeSIP, it is important to quantify signaling cost. Similar to that in [26], [27], [28], [29], the signaling cost function comprises transmission cost and processing cost. The transmission cost is proportional to the distance between the two network nodes. The processing cost includes the cost to process messages, verify messages, and so on.

In our proposed SeSIP, the inter-realm roaming of a mobile network includes three types of handoff: 1) From the intranet (home network) to a foreign network, 2) From a foreign network to another foreign network, and 3) From a foreign network back to the intranet.

They are represented as H_{hf} , H_{ff} and H_{fh} , respectively.

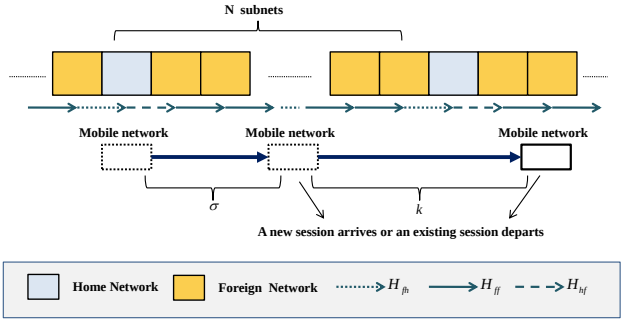

Figure 10. Network topology for analysis

We assume that the network topology is configured as shown in Fig. 10 such that the mobile network returns to the intranet after it moves across *N–1* foreign networks. Hence, when *N* is larger, the mobile network travels far away from its home network before it returns [40]. For example, the handoff sequence can be shown as $H_{hf}H_{ff}H_{ff}...H_{ff}H_{fh}$. Table 2 lists the parameters used in the analysis.

For a mobile network, let $f_m(t)$ be a general density function for the network residence time t_M in a subnet.

Let $E[t_M]=1/\gamma$. Its Laplace transform is written:

$$f_m^*(s)=\int_{t=0}^{\infty} e^{-st} f_m(t)dt.$$

Table 2. Parameter Definitions for Each Subsystem i .

Parameter	Definition
N	Number of networks a mobile network visits before it goes back to the intranet.
λ	Session arrival rate for a mobile network
$1/\mu$	Average session service time
$1/\gamma$	Average network residence time

c	Maximum number of ongoing sessions in a mobile network
δ_σ	Probability density function of σ

We assume that the arrival of SIP sessions to the mobile network follows a Poisson process with arrival rate λ. The service time of a session is exponentially distributed with mean $1/\mu$. As shown in the diagram in Fig. 9, similar to that in [30], we define $a(k)$ as the probability that a mobile network will move across k subnets between two events while there are i ongoing sessions in the mobile network. An event here is a new session arrival or an ongoing session departure from the mobile network. We denote $E\left[t_{S_i}\right]$ as the interval between two consecutive events. During $E\left[t_{S_i}\right]$ there are i ongoing sessions in the mobile network. Based on the property of sums of two independent Poisson process, $E\left[t_{S_i}\right]$ can be considered as the inter arrival time of a new Poisson process. Therefore,

$$E\left[t_{S_i}\right]=\frac{1}{\pi}=\begin{cases}\dfrac{1}{\lambda+i\mu}, & 0\le i<c\\ \dfrac{1}{i\mu}, & i=c,\end{cases} \tag{1}$$

where c is the maximum number of ongoing sessions allowed in a mobile network. According to the above assumption, we have:

$$a_i(k)=\begin{cases}1-\dfrac{(1-f_m^*(\pi_i))\gamma}{\pi_i}, & k=0,\\ \dfrac{\gamma}{\pi_i}\left[1-f_m^*(\pi_i)\right]^2\left[f_m^*(\pi_i)\right]^{k-1}, & k>0.\end{cases} \tag{2}$$

For simplicity, we denote $g_i=f_m^*(\pi_i)$ in the rest of the paper. Let $k=jN+q$ and $0\le q<N$. Then,

$$a_i(jN+q)=\frac{\gamma(1-g_i)^2}{\pi_i g_i}(g_i^N)^j g_i^q=yz^j x^q, \tag{3}$$

For demonstration purpose, we assume that the network residence time follows a Gamma distribution. The Laplace transform of a Gamma random variable is expressed:

$$f_m^*(s)=\left(\frac{\gamma\beta}{s+\gamma\beta}\right)^\beta. \tag{4}$$

Hence, we obtain:

$$g_i=f_m^*(\pi_i)=\left(\frac{\gamma\beta}{\pi_i+\gamma\beta}\right)^\beta. \tag{5}$$

In the proposed SeSIP, when a mobile network moves across networks, it must perform registration with the SIP Registrar to update its location. It also must send re-INVITE messages to the CNs if there are ongoing sessions with the MNs in the mobile network. Hence, the cost comprises two parts: the registration cost for SIPNVG and the re-INVITE cost for maintaining session continuity. The registration cost is independent of the number of ongoing sessions in the mobile network, because the SIP-NVG can register with the SIP Registrar on behalf of the whole mobile network. On the other hand, the re-INVITE cost depends on the number of ongoing sessions in the mobile network.

The cost increases when the number of ongoing sessions increases. However, because we design a URI list embedded in one re-INVITE message, the cost to really send a re-INVITE message to each individual CN is nearly constant, regardless of the number of ongoing sessions in the mobile network. Moreover, client authentication is performed through one handshake by using HOTP-based authentication [5] when the REGISTER or INVITE is requested. This reduces the request/response number when the signaling message is processed, thereby reducing the processing cost of the signaling. This can be seen in Fig. 6, 8, and 9. Table 3 lists the parameters for handoff signaling cost.

Therefore, we can denote the signaling cost for handoff:

$$\begin{aligned}S_{hf}^i&=R_f+L_{hf}+iI_{hf},\\ S_{ff}^i&=R_f+L_{ff}+iI_{ff},\\ S_{fh}^i&=R_h+L_{fh}+iI_{fh}.\end{aligned} \tag{6}$$

During $E\left[t_{S_i}\right]$, we assume that the mobile network crosses *k* subnets as shown in Fig. 10. We define σ as the number of subnets the mobile network moved across from the time it visited the intranet until the time the last event occurred. When $0 < \sigma <$ N, the total signaling cost in the mobile network during $E\left[t_{S_i}\right]$ can be derived as :

Table 3. Parameters for Handoff Signalling Cost.

Parameter	Definition
S_{hf}^{i}	Average handoff cost when a mobile network moves from the home network to a foreign network with i ongoing sessions.
S_{ff}^{i}	Average handoff cost when a mobile network moves from a foreign network to another foreign network with i ongoing sessions.
S_{fh}^{i}	Average handoff cost when a mobile network moves from a foreign network to the home network with i ongoing sessions.
R_h	Average registration cost of a mobile network (sent by SIP-NVG) when the mobile network enters its home network.
R_f	Average registration cost of a mobile network (sent by SIP-NVG) when the mobile network enters a foreign network.
L_{hf}	Average cost for the first part of re-INVITE when a mobile network moves from its home network to a foreign network.
L_{ff}	Average cost for the first part of re-INVITE when a mobile network moves from a foreign network to another foreign network.
L_{fh}	Average cost for the first part of re-INVITE when a mobile network moves from a foreign network to its home network.
I_{hf}	Average cost for the second part of re-INVITE of a session when a mobile network moves from its home network to a foreign network.
I_{ff}	Average cost for the second part of re-INVITE of a session when a mobile network moves from a foreign network to another foreign network.
I_{fh}	Average cost for the second part of re-INVITE of a session when a mobile network moves from a foreign network to its home network.

$$
\begin{aligned}
&C_i(N,\pi_i,\gamma,\sigma) = \\
&\sum_{k=0}^{\infty}\left\{S_{hf}^{i}\left[\frac{k+\sigma-1}{N}\right]+S_{fh}^{i}\left[\frac{k+\sigma}{N}\right]+\right. \\
&\left.S_{ff}^{i}\left(k-\left[\frac{k+\sigma-1}{N}\right]-\left[\frac{k+\sigma}{N}\right]\right)\right\}a_i(k) \\
&= S_{ff}^{i}\frac{\gamma}{\pi_i}+\frac{(S_{hf}^{i}g_i-S_{ff}^{i}g_i+S_{fh}^{i}-S_{ff}^{i})(1-g_i)g_i^{N-1}\gamma}{(1-g_i^{N})g_i^{\sigma}\pi_i}. \quad (7)
\end{aligned}
$$

If σ is exponentially distributed, the *p.d.f* of σ is:

$$
\delta_\sigma = \begin{cases} e^{-\sigma}\left(\dfrac{1-2e^{-(N+1)/2}+e^{-1}}{1-e^{-1}}\right), & 0 \le \sigma < \dfrac{N-1}{2} \\ e^{-(N-\sigma)}\left(\dfrac{1-2e^{-(N+1)/2}+e^{-1}}{1-e^{-1}}\right), & \dfrac{N-1}{2} < \sigma \le N-1. \end{cases} \quad (8)
$$

Therefore,

$$
\begin{aligned}
&C_{i\_exponential}(N,\pi_i,\gamma) = \\
&\sum_{\sigma=0}^{N-1}\delta_\sigma C_i(N,\pi_i,\gamma,\sigma) = S_{ff}^{i}\frac{\gamma}{\pi_i}+\frac{\gamma(1-g_i)}{\pi_i(1-g_i^{N})} \\
&\left\{\frac{(1-e^{-1})(S_{hf}^{i}-S_{ff}^{i}+(S_{fh}^{i}-S_{ff}^{i})g_i^{N-1})}{1-2e^{-(N+1)/2}+e^{-1}}+\right. \\
&\frac{(1-e^{-1})(S_{hf}^{i}g_i-S_{ff}^{i}g_i+S_{fh}^{i}-S_{ff}^{i})g_i^{N-1}}{1-2e^{-(N+1)/2}+e^{-1}} \\
&\left.\left(\sum_{\sigma=1}^{(N-1)/2}\frac{e^{-\sigma}}{g_i^{\sigma}}+\sum_{\sigma=(N+1)/2}^{N-1}\frac{e^{-(N-\sigma)}}{g_i^{\sigma}}\right)\right\} \quad (9)
\end{aligned}
$$

As discussed above, the arrival of sessions to a mobile network follows a Poisson process, and the session service time is exponentially distributed. In addition, there is a limit *c* for the maximum number of ongoing sessions allowed in the mobile network. Therefore, we can model the number of ongoing sessions in a mobile network as an *M/M/c/c* queuing system. The steady state probability that there are *i* ongoing sessions in the mobile network is then given by [31]:

$$
P_i = \frac{\lambda^{i}}{i!\mu^{i}}\left(\sum_{x=0}^{c}\frac{\lambda^{x}}{x!\mu^{x}}\right)^{-1} \quad (10)
$$

As a result, the average handoff-signaling cost per unit time can be derived as:

$$
\sum_{i=0}^{c}C_{i\_exponential}P_i\pi_i. \quad (11)
$$

The variables π_i and P_i can be obtained from (1) and (10). Further, we consider the effect of the variance of the mobility pattern. We assume the average residence time is gamma distributed [32], [33]. Therefore, the variance is:

$$Var = \frac{1}{\beta\gamma^2} \tag{12}$$

Table 4. Parameters for SeSIP Signalling Cost.

Parameter	Definition
a_x	The processing cost for SIP registration at Node x
b_x	The processing cost for SIP INVITE message at Node x
$A_{x,y}$	The transmission cost of SIP registration between Node x and Node y
$B_{x,y}$	The transmission cost of a SIP INVITE message between Node x and Node y
U	The total cost for SIP Proxy 1 to process and transmit UAR/UAA messages to the Diameter server
M	The total cost for SIP Proxy 2 to process and transmit MAR/MAA messages to the Diameter server

To evaluate the performance of the proposed SeSIP, Table 4 lists the parameters used in SeSIP Signaling Cost. where *x* and *y* can be *mn; nvg; pro; reg; alg*; or *cn* which denote MN, SIP-NVG, SIP Proxy 1, SIP Proxy 2 (SIP Registrar), ALG, and CN, respectively. According to the signaling message flow described in Section 3, the above costs can be calculated:

$$\begin{aligned}
R_h &= a_{nvg} + a_{reg} + 2A_{nvg,reg} + M,\\
R_f &= a_{nvg} + 2a_{pro} + a_{reg} + 2A_{nvg,pro} + 2A_{pro,reg} + U + M,\\
L_{hf} &= 2b_{nvg} + 3b_{pro} + 4b_{reg} + 2b_{alg} + 3B_{nvg,pro} + 3B_{pro,reg}\\
&\quad + 4B_{reg,alg} + B_{reg,cn} + M,\\
L_{ff} &= 2b_{nvg} + 3b_{pro} + 2b_{reg} + b_{alg} + 3B_{nvg,pro} + 3B_{pro,reg}\\
&\quad + 2B_{reg,alg} + M,\\
L_{fh} &= 2b_{nvg} + 3b_{reg} + b_{alg} + 3B_{nvg,reg} + 2B_{reg,alg} + B_{reg,cn}\\
&\quad + M,\\
I_{hf} &= b_{mn} + b_{nvg} + b_{reg} + b_{cn} + 2B_{mn,nvg} + 2B_{reg,cn},\\
I_{ff} &= b_{mn} + b_{nvg} + 2B_{mn,nvg},\\
I_{fh} &= b_{mn} + b_{nvg} + 2B_{mn,nvg} + b_{reg} + b_{cn} + 2B_{reg,cn};
\end{aligned}$$

To compare the signaling cost to that of IETF MVPN, we assume the Diameter MIPv4 application [34] is used to authenticate the *x*-MIP. Also, we assume MN is in collocated mode. Analysis of an FA mode is not presented here, because it has almost the same results. The subscripts *mn;mg; vpn; xha*; and *iha* refer to MN, Mobile Gateway, IPsec-based VPN gateway, *x*-HA, and *i*-HA, respectively. Also, the following parameters are defined: Based on the signaling message flow shown in Fig. 2, the above cost can be calculated:

$$\begin{aligned}
M_x &= 2d_{mg} + 2d_{xha} + 2W_{mn,mg} + 2W_{mg,xha} + 2H,\\
M_{i-o} &= 2d_{mg} + 2d_{xha} + 2d_{vpn} + d_{iha} + 2W_{mn,mg}\\
&\quad + 2W_{mg,xha} + 2W_{xha,vpn} + 2W_{vpn,iha} + 2H,\\
M_{i-i} &= d_{iha} + 2W_{mn,mg} + 2W_{mg,iha},\\
T_{est} &= 2e_{mn} + 6e_{mg} + 6e_{xha} + 3e_{vpn} + 6Z_{mn,mg}\\
&\quad + 6Z_{mg,xha} + 6Z_{xha,vpn},\\
T_{ter} &= Z_{mn,mg} + Z_{mg,vpn} + e_{vpn}.
\end{aligned}$$

The handoff cost of IETF MVPN when a mobile network moves between networks is derived as:

$$\begin{aligned}
D_{hf} &= M_x + M_{i-o} + T_{est},\\
D_{ff} &= M_x,\\
D_{fh} &= M_{i-i} + T_{ter}.
\end{aligned} \tag{13}$$

In the architecture we propose, SIP-NVG manages the overall network mobility, registering the whole mobile network in the SIP Registrar when it moves to a new subnet. If there is no SIP-NVG, all MNs in the same mobile network must update their locations separately. This increases signaling cost. We can re-define the costs (6) when there is no SIP-NVG as follows:

$$\begin{aligned}
S^i_{hf} &= mR_f + iL_{hf} + iI_{hf},\\
S^i_{ff} &= mR_f + iL_{fh} + iI_{ff},\\
S^i_{fh} &= mR_h + iL_{hh} + iI_{fh}.
\end{aligned} \tag{14}$$

where *m* is the number of MNs connected to the mobile network. In addition, the HOTP authentication method [5] used in the proposed architecture is an event synchronization method that performs client authentication through a single handshake. In contrast, the HTTP digest authentication method adopted by many other security protocols is based on the challenge-response paradigm and requires two handshakes between the client of the SIP server and the Diameter server. This is because the SIP Registrar

uses UAR/UAA and MAR/MAA commands for the Diameter server for user authentication and authorization when the client of the SIP server transmits SIP REGISTER and INVITE messages. Therefore, the cost incurred in the use of HTTP digest authentication can be calculated as follows:

$$R_h = 2a_{nvg} + 2a_{reg} + 4A_{nvg,reg} + 2M,$$

$$R_f = 2a_{nvg} + 4a_{pro} + 2a_{reg} + 4A_{reg,pro} + 4A_{pro,reg} + 2U + 2M,$$

$$L_{hf} = 3b_{nvg} + 5b_{pro} + 5b_{reg} + 2b_{alg} + 5B_{reg,pro} + 5B_{pro,reg} + 4B_{reg,alg} + B_{reg,cn} + 2M,$$

$$L_{ff} = 3b_{nvg} + 5b_{pro} + 3b_{reg} + b_{alg} + 5B_{reg,pro} + 5B_{pro,reg} + 2B_{reg,alg} + 2M,$$

$$L_{fh} = 3b_{nvg} + 4b_{reg} + b_{alg} + 5B_{nvg,reg} + 2B_{reg,alg} + B_{reg,cn} + 2M,$$

$$I_{hf} = b_{mn} + b_{nvg} + b_{reg} + b_{cn} + 2B_{mn,nvg} + 2B_{reg,cn},$$

$$I_{ff} = b_{mn} + b_{nvg} + 2B_{mn,nvg},$$

$$I_{fh} = b_{mn} + b_{nvg} + b_{reg} + b_{cn} + 2B_{mn,nvg} + 2B_{reg,cn}.$$

4.2 Numerical Results

This section provides the numerical results for the analysis presented in Section 4. The analysis was validated by extensive simulations using *ns-2* [35]. As discussed in Section 4, the signaling cost function consists of the transmission cost and the processing cost. We assume that the transmission cost is proportional to the distance between the source and destination nodes, and the processing cost includes the processing and verifying SIP messages [36], [37], [38], [39]. Also, the transmission cost of a wireless link is higher than that of a wire line. To illustrate performance, reasonable values were chosen for the parameters, as listed in Table 5. Additionally, to compare our designs signaling cost with that of IETF MVPN, we assumed the *x*-HA was optimally collocated with the VPN gateway and AAAF, and the *i*-HA was collocated with the SIP Proxy 2/Registrar.

Also, the AAAH in IETF MVPN as collocated with the Diameter server in the SeSIP. One of the major objectives in the proposed SeSIP is to reduce the signaling cost for handoff while supporting the VPN.

Table 5. Table Type Styles.

Parameter	Definition
M_x	The x-MIP registration cost.
M_{i-o}	The i-MIP registration cost when MN is located outside the intranet.
M_{i-i}	The i-MIP registration cost when MN is located inside the intranet.
T_{est}	The establishment cost of IPsec tunnel.
T_{ter}	The termination cost of IPsec tunnel.
d_x	The processing cost for MIP registration at Node x.
e_x	The processing cost for IPsec message at Node x.
$W_{x,y}$	The transmission cost of MIP registration between Node x and Node y.
$Z_{x,y}$	The transmission cost of IPsec message between Node x and Node y.
H	The total cost for x-HA to process and transmit HAR/HAA and AMR/AMA messages to AAAF and AAAH.

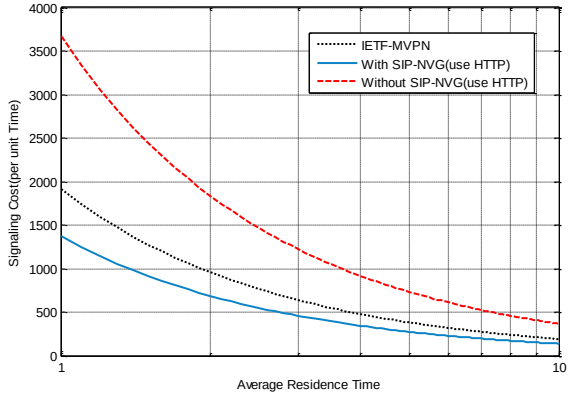

Figure 11. Comparison of various signalling costs versus residence time(1)

Fig. 11 presents a comparison among the signaling costs with IETF MVPN, with and without SIP-NVG using HTTP. Also Fig. 12 presents a comparison among the signaling costs with SIP-NVG using HTTP, and using HOTP. As defined above, *m* is the number of MNs attached to the mobile network. In addition, we assume $N = 7$, $m = 5$, $c = 10$, and $\rho = \rho/\mu = 5$. In the SIP-based protocol, SIP re-INVITEs and SIPs registration must be performed during each handoff. Therefore, the signaling cost for a SIP-based protocol might be higher than for MIP. However, Fig. 11 shows that a method with SIP-NVG has lower signaling costs for handoff than in IETF MVPN. This is because IETF MVPN

requires time to establish the three tunnels. Compared to the mobile network without SIP-NVG, the method with SIP-NVG reduces handoff signaling cost significantly, since SIP-NVG performs registration in the SIP Registrar on behalf of the entire mobile network when it moves to a new subnet, whereas, without SIP-NVG, all MNs must update their locations individually.

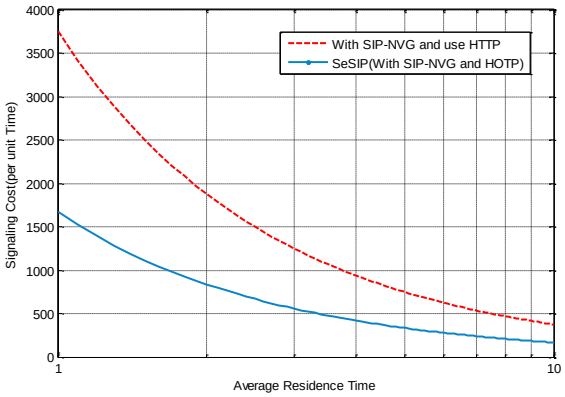

Figure 12. Comparison of various signalling costs versus residence time(2)

And, Fig. 12 shows that SeSIP(with SIP-NVG using HOTP) has lower signaling costs for handoff than in SIP-NVG using HTTP. Further, our results show that the HOTP authentication method reduces signaling cost, compared to the HTTP digest authentication method, by reducing the required handshakes from two to one. Handoff signaling cost decreases when the average network duration time increases, i.e., when the mobile network has relatively low mobility. Fig. 13, 14 demonstrates the average signaling cost for handoff versus ρ, the number of sessions in the mobile network. The parameters are set as in Fig. 11, 12 except that $\gamma = 0.1$. Similar to Fig. –11, 12, the proposed SeSIP has less signaling cost for handoff than without SIP-NVG using HOTP or with SIP-NVG using the HTTP digest method. We also that when ρ increases, the average cost for SIP-based solutions increases too. The reason is that with more ongoing sessions, more re-INVITEs are needed to maintain session continuity. Besides, when ρ is larger than 20, the costs of all techniques presented in Fig. 13, 14 remain almost constant. This is because, when ρ approaches 20, the number of ongoing sessions with each technique reaches the maximum number allowed in the mobile network. Comparing $c = 10$ and $c = 15$ in the SIP-based techniques, more sessions exist in the mobile network when $c = 10$. Hence, greater signaling cost occurs for a re-INVITE. Because moving from home network to foreign network causes higher signaling cost than other types of handoffs, revisiting the home network frequently results in higher signaling cost.

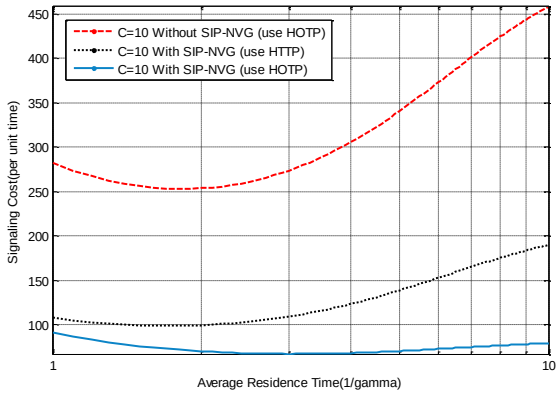

Figure 13. Comparison of signalling cost with and without SIP-NVG and using HTTP or HOTP Method (C=10)

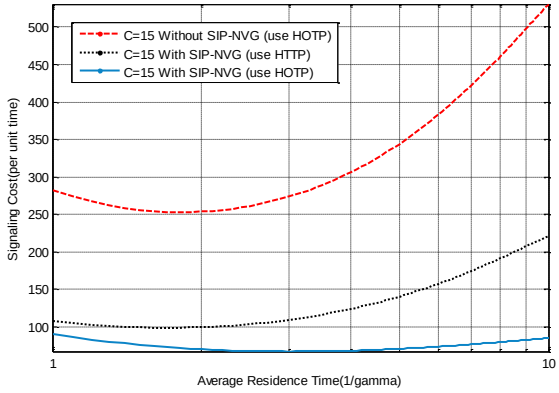

Figure 14. Comparison of signalling cost with and without SIP-NVG and using HTTP or HOTP Method (C=15)

5 CONCLUSIONS

Although the IETF standard has proposed a mobile VPN architecture, it is designed for the movement of a signal node only. In addition, IETF MVPN has large overhead for transmitting real-time packets, because it requires one IPsec tunnel and two MIP tunnels. On the other hand, there has been no efficient way to support mobile VPN in NEMO, even though NEMO supports network mobility. This paper presents a novel method for supporting MVPN in NEMO that ensures that the

session is maintained continuously when the whole network moves, and it proposes using the HOTP-based authentication method to shorten the processing time of the signaling that continuously occurs to maintain the session. In addition, security is enhanced in our design through the integration of NEMO and VPN.

We analyzed the design and performance of our proposed design, and results indicate that the proposed SeSIP based on SIP is well suited to real-time service. Although SIP-based mobility management can easily support routing optimization, there may be an upswing in the handoff signaling costs, because many signaling messages are transmitted to maintain the session in progress with SIP in NEMO. In the proposed SeSIP, a URI list is used to signify the SIP proxy server instead of transmitting signaling messages individually to each node. Therefore, the signaling cost is reduced. User authentication using the existing HTTP digest authentication method requires many handshakes, increasing the signaling cost. In contrast, the proposed SeSIP using HOTP-based authentication considerably reduces the number of handshakes needed with the authentication server, thus reducing the signaling cost. The SIP proxy server and the Diameter server are responsible for authentication and authorization. Also, the ALG receives a command from the SIP proxy server to process the security information for the data transmission, depending on MIDCOM architecture. ALG is responsible for converting and relaying the protected and unprotected data. Thus, unauthorized data cannot pass the ALG in the Internet. This paper examined a method for efficient management of group mobility and cost savings for real-time services through the integration of mobile VPN and NEMO. NEMO, currently in the early stage of research, is expected to be further realized through the convergence of various technologies, policies, and methods, such as the path optimization method for efficient services, multi-homing technology, and methods for services in the inclusive mobility network.

These need to be researched in the period ahead. For commercial service, research should also be conducted to develop technology to enable fast detection of movement.

6 ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2010-0024695).

This article is a revised and expanded version of a paper entitled ‘Secure SIP-based Mobility Management Scheme for Cost-Optimized NEMO Environments’ presented at The International Conference on Digital Information, Networking, and Wireless Communications (DINWC2014) held on June 24-66, 2014 at Ostrava, Czech Republic.

7 REFERENCES

[1] V. Schena and G. Losquadro, FIFTH Project Solutions Demonstrating New Satellite Broadband Communication System for High Speed Train, Proc. IEEE Vehicular Technology Conf., pp. 2831-2835, May 2004.

[2] WirelessCabin Project, http://www.wirelesscabin.com, 2011.

[3] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, Network Mobility (NEMO) Basic Support Protocol, IETF RFC 3963, Jan. 2005.

[4] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, IETF RFC 2401, Nov. 1998.

[5] D. MRaihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen,HOTP: An HMAC-Based One-Time Password Algorithm,RFC 4226, December 2005.

[6] S. Vaarala and E. Klovning, Mobile IPv4 Traversal Across IPsec-Based VPN Gateways, IETF RFC 5265, June 2008. 7.

[7] D. Harkins and D. Carrel, The Internet Key Exchange (IKE),IETF RFC 2409, Nov. 1998.

[8] J.-C. Chen, Y.-W. Liu, and L.-W. Lin, Mobile Virtual Private Networks with Dynamic MIP Home Agent Assignment, Wireless Comm. and Mobile Computing, vol. 6, no. 5, pp. 601-616, Aug. 2006.

[9] J.-C. Chen, J.-C. Liang, S.-T. Wang, S.-Y. Pan, Y.-S. Chen, and Y.-Y. Chen, Fast Handoff in Mobile Virtual Private Networks, Proc. IEEE Intl Symp. World of Wireless Mobile and Multimedia Networks (WoWMoM 06), pp. 548-552, June 2006.

[10] S.-C. Huang, Z.-H. Liu, and J.-C. Chen, SIP-Based Mobile VPN for Real-Time Applications, Proc. IEEE Wireless Comm. And Networking Conf. (WCNC 05), pp. 2318-2323, Mar. 2005.

[11] Z.-H. Liu, J.-C. Chen, and T.-C. Chen, Design and Analysis of SIP-Based Mobile VPN for Real-Time Applications, IEEE Trans. Wireless Comm., vol. 8, no. 11, pp. 5650-5661, Nov. 2009.

[12] A. Dutta, F. Vakil, J.-C. Chen, M. Tauil, S. Baba, N. Nakajima, and H. Schulzrinne, Application Layer Mobility Management Scheme for Wireless Internet, Proc. IEEE Intl Conf. Third Generation Wireless and beyond (3G Wireless), pp. 379-385, May 2001.

[13] D. Vali, S. Paskalis, A. Kaloxylos, and L. Merakos, An Efficient Micro-Mobility Solution for SIP Networks, Proc. IEEE GLOBECOM, pp. 3088-3092, Dec. 2003.

[14] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, The Secure Real-Time Transport Protocol (SRTP),IETF RFC 3711, Mar. 2004.

[15] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, MIKEY: Multimedia Internet KEYing, IETF RFC 3830, Aug. 2004.

[16] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko,Diameter Base Protocol, IETF RFC 3588, Sept. 2003.

[17] M. Garcia-Martin, M. Belinchon, M. Pallares-Lopez, C. Canales, and K. Tammi, Diameter Session Initiation Protocol (SIP) Application, IETF RFC 4740, Nov. 2006.

[18] P. Srisuresh, J. Kuthan, J. Rosenberg, A. Molitor, and A. Rayhan, Middlebox Communication Architecture and Framework, IETF RFC 3303, Aug. 2002.

[19] M. Handley and V. Jacobson, SDP: Session Description Protocol, IETF RFC 2327, Apr. 1998.

[20] J.-C. Chen and T. Zhang, IP-Based Next-Generation Wireless Networks. John Wiley and Sons, Jan. 2004.

[21] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, RTP: A Transport Protocol for Real-Time Applications, IETF RFC 3550, July 2003.

[22] E. Rescorla, SSL and TLS: Designing and Building Secure Systems. Addison Wesley, 2001.

[23] D. Geneiatakis, G. Kambourakis, C. Lambrinoudakis, T. Dagiuklas, and S. Gritzalis, A Framework for Protecting a SIP-Based Infrastructure against Malformed Message Attacks, Computer Networks, vol. 51, no. 10, pp. 2580-2593, July 2007.

[24] D. Geneiatakis and C. Lambrinoudakis, An Ontology Description for SIP Security Flaws, Computer Comm., vol. 30, no. 6, pp. 1367-1374, Mar. 2007.

[25] D. Geneiatakis, G. Kambourakis, and T. Dagiuklas, A Framework for Detecting Malformed Messages in SIP Networks, Proc. 14th IEEE Workshop Local and Metropolitan Area Networks, 5 pp. -5, Sept. 2005.

[26] J. Xie and I.F. Akyildiz, A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP, IEEE Trans. Mobile Computing, vol. 1, no. 3, pp. 163-175, July-Sep. 2002.

[27] W. Ma and Y. Fang, Dynamic Hierarchical Mobility Management Strategy for Mobile IP Networks, IEEE J. Selected Areas Comm., vol. 22, no. 4, pp. 664-676, May 2004.

[28] R. Rummler, Y.W. Chung, and A.H. Aghvami, Modeling and Analysis of an Efficient Multicast Mechanism for UMTS, IEEE Trans. Vehicular Technology, vol. 54, no. 1, pp. 350-365, Jan. 2005.

[29] S. Fu, M. Atiquzzaman, L. Ma, and Y.-J. Lee, Signaling Cost and Performance of SIGMA: A Seamless Handover Scheme for Data Networks, Wireless Communications and Mobile Computing, vol. 5, no. 7, pp. 825-845, Nov. 2005.

[30] Y.-B. Lin, Reducing Location Update Cost, IEEE/ACM Trans. Networks, vol. 5, no. 1, pp. 25-33, Feb. 1997.

[31] D. Gross and C.M. Harris, Fundmentals of Queueing Theory. John Wiley and Sons, 1998.

[32] M.M. Zonoozi and P. Dassanayake, User Mobility Modeling and Characterization of Mobility Patterns, IEEE J. Selected Areas Comm., vol. 15, no. 7, pp. 1239-1252, Sept. 1997.

[33] Y. Fang and I. Chlamtac, Teletraffic Analysis and Mobility Modeling of PCS Networks, IEEE Trans. Comm., vol. 47, no. 7, pp. 1062-1072, July 1999.

[34] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, and P. McCann, Diameter Mobile IPv4 Application, RFC 4004, Aug. 2005.

[35] The Network Simulator- ns-2, http://www.isi.edu/nsnam/ns, 2011.

[36] J. Xie and I.F. Akyildiz, A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP, IEEE Trans. Mobile Computing, vol. 1, no. 3, pp. 163-175, July-Sep. 2002.

[37] W. Ma and Y. Fang, Dynamic Hierarchical Mobility Management Strategy for Mobile IP Networks, IEEE J. Selected Areas Comm., vol. 22, no. 4, pp. 664-676, May 2004.

[38] R. Rummler, Y.W. Chung, and A.H. Aghvami, Modeling and Analysis of an Efficient Multicast Mechanism for UMTS, IEEE Trans. Vehicular Technology, vol. 54, no. 1, pp. 350-365, Jan. 2005.

[39] S. Fu, M. Atiquzzaman, L. Ma, and Y.-J. Lee, Signaling Cost and Performance of SIGMA: A Seamless Handover Scheme for Data Networks, Wireless Communications and Mobile Computing, vol. 5, no. 7, pp. 825-845, Nov. 2005.

[40] T.C. Chen, J.C. Chen, Z.H. Liu, "Secure Network Mobility (SeNEMO) for Real-Time Applications," IEEE Trans. Mobile Computing, vol. 10, no. 8, Aug 2011.