



ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Secure Network Mobility (SeNEMO) based on SIP

A. Sivanesh Kumar A.P, and Dr.V. Khana

Dean, Bharath University

ARTICLE INFO

Article history:

Received 28 January 2015

Accepted 25 February 2015

Available online 6 March 2015

Keywords:

NEMO, MVPN, SIP, HOTP, Mobility Management

ABSTRACT

Mobile Virtual Private Network (VPN) has been developed to secure mobile user's communication between untrusted external networks and the protected private internal network. However, the IETF's mobile VPN does not address how to support NEMO. Existing secure network has been developed architecture to support VPN in NEMO. The tunnels increase massive overhead in terms of packets length and processing time. This may degrade the performance of real-time applications, which are sensitive to bandwidth and delay. In addition, it is not suitable for real-time applications. The predefined cryptographic transformations provide low computational cost and limited packet expansion so bandwidth can be used more economically than IPsec. We present sensing mechanisms that can be used for implicit high-load and overload detection in SIP networks. By means of measurements and implements we highlight the characteristics of SIP proxy servers for different load situations and using different transport protocols. Each protocol yields to distinctive patterns that encourage deriving an algorithm that is able to estimate a downstream server's current load. In this work, we propose architecture and protocols to support VPN in NEMO, which is called Secure NEMO (SeNEMO). The proposed SeNEMO, based on Session Initiation Protocol (SIP), is specifically designed for real-time applications over VPN. It allows an entire network to move and still maintains session continuity. In addition to analyzing the security vulnerabilities, we also propose analytical models to evaluate the performance of the proposed SeNEMO.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: A. Sivanesh Kumar A.P, and Dr.V. Khana, Secure Network Mobility (SeNEMO) based on SIP. *Aust. J. Basic & Appl. Sci.*, 9(10): 59-64, 2015

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 (Schena, 2004; Wireless Cabin Project, 2001; Devarapalli, 2005). 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 (Kent, 1998) 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) (MRaihi, 2005) 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.

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.

Related work:

IETF has previously defined the architecture and protocol for MVPN (Vaarala, 2008) 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) (Harkins, 1998). Fig. 1 shows the three tunnels (x-MIP, IPsec, and i-MIP).

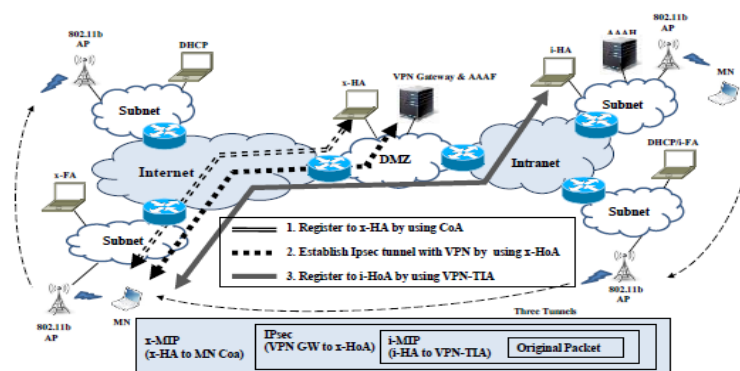


Fig. 1: MVPN proposed by IETF.

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 (Chen, 2006; Chen, 2006). 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 (Huang, 2005).

In this paper, we propose SIP-based NEMO because it is easily distributed and reduces the data transfer delay for host and session mobility (Wireless Cabin Project, 2001; Devarapalli, 2005). 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.

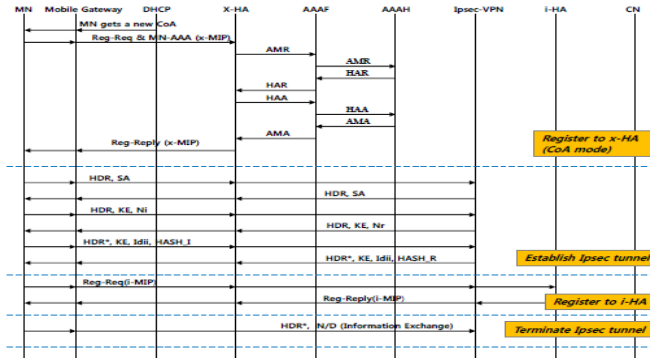


Fig. 2: Signalling flows of IETF MVPN.

Cost-effective and secure mobility management scheme:

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 (Huang, 2005). The proposed SeSIP comprises SIP, secure real-time transport protocol (SRTP) (Harkins, 1998), multimedia internet keying (MIKEY) (MRaihi, 2005) and a Diameter server (Vaarala, 2008) to provide VPN services in NEMO. Fig. 3 depicts the architecture of the proposed SeSIP

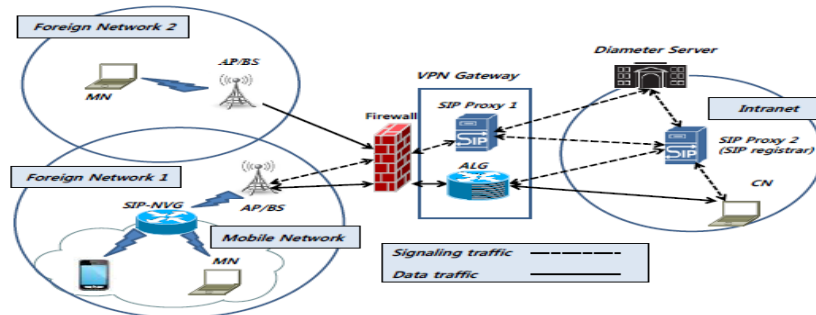


Fig. 3: System architecture.

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 (Harkins, 1998) is an adaptation of the Diameter base protocol (Vaarala, 2008) 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) (Chen, 2006). In addition, MIKEY messages are embedded inside the messages of the Diameter base protocol and the Session Description Protocol (SDP) (Chen, 2006) 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. 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 MN's new location. SRTP defines a framework to provide encryption and integrity for Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) 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 (TKG) 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 (MRaihi, 2005) 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.

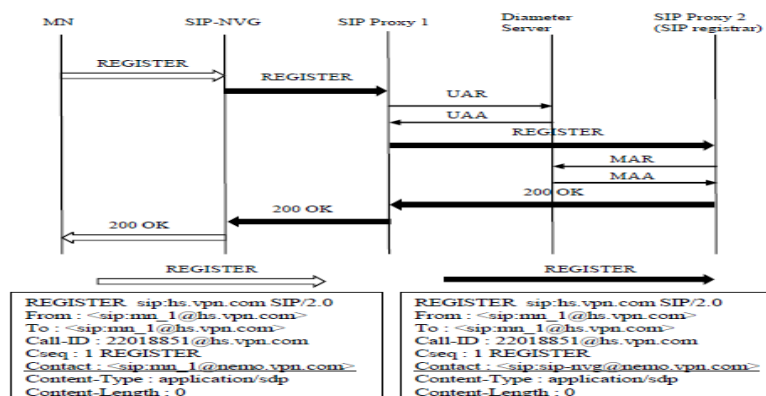


Fig. 4: Message flows and translation of REGISTER when mobile network resides in foreign network.

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.

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 MN's address into the SIP-NVG's 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.

Numerical results:

This section provides the numerical results for the analysis. The analysis was validated by extensive simulations using *ns-2*.

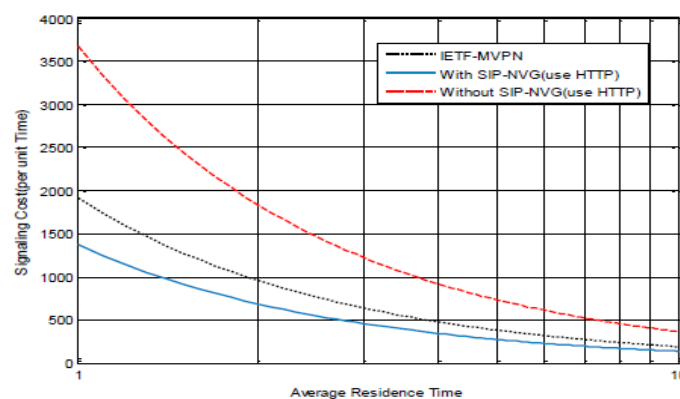


Fig. 5: Comparison of various signalling costs versus residence time(1).

Fig. 5 presents a comparison among the signaling costs with IETF MVPN, with and without SIP-NVG using HTTP. However, Fig. 5 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.

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.

REFERENCES

- Chen, J.C., J.C. Liang, S.T. Wang, S.Y. Pan, Y.S. Chen and Y.Y. Chen, 2006. Fast Handoff in Mobile Virtual Private Networks, Proc. IEEE Intl Symp. World of Wireless Mobile and Multimedia Networks (WoWMoM 06), pp: 548-552.
- Chen, J.C., Y.W. Liu and L.W. Lin, 2006. Mobile Virtual Private Networks with Dynamic MIP Home Agent Assignment, Wireless Comm. and Mobile Computing, 6(5): 601-616.
- Devarapalli, V., R. Wakikawa, A. Petrescu, and P. Thubert, 2005. Network Mobility (NEMO) Basic Support Protocol, IETF RFC 3963, Jan.
- Harkins, D. and D. Carrel, 1998. The Internet Key Exchange (IKE), IETF RFC 2409.
- Huang, S.C., Z.H. Liu, and J.C. Chen, 2005. SIP-Based Mobile VPN for Real-Time Applications, Proc. IEEE Wireless Comm. And Networking Conf. (WCNC 05), pp: 2318-2323.
- Kent, S. and R. Atkinson, 1998. Security Architecture for the Internet Protocol, IETF RFC 2401, Nov.
- MRaihi, D., M. Bellare, F. Hoornaert, D. Naccache and O. Ranen, 2005. HOTP: An HMAC-Based One-Time Password Algorithm, RFC 4226.
- Schena, V. and G. Losquadro, 2004. FIFTH Project Solutions Demonstrating New Satellite Broadband Communication System for High Speed Train, Proc. IEEE Vehicular Technology Conf., pp: 2831-2835.
- Vaarala, S. and E. Klovning, 2008. Mobile IPv4 Traversal Across IPsec-Based VPN Gateways, IETF RFC 5265, June 2008. 7.
- Wireless Cabin Project, 2001. <http://www.wirelesscabin.com>.