Session Initiation Protocol for Security in Mobile Networks

P. Thamaraikannan and P. Vijayaragavan

Abstract--- *The Network Mobility working group has considered how to enable an entire network using IETF to move from one location to another without any session lost. Mobile Virtual Private Network (MVPN) has been developed to mobile user's communication between external networks and the protected private internal mobile network. The IETF's mobile VPN does not address how to support Network Mobility. In addition, VPN is not suitable for real-time applications in Mobile Network. This project proposes an architecture and Session Initiation Protocol (SIP) to support VPN in Network Mobility, which is called Secure Network Mobility. The proposed Secure Network Mobility, based on SIP, is specifically designed for real-time applications over MVPN. It allows an entire network to move and still maintains session continuity with security features. In addition to analyzing the security vulnerabilities, this is also proposing analytical models to evaluate the performance of the proposed Secure Network Mobility for Performance analysis. Finally results show that the proposed Secure Network Mobility can reduce signaling cost significantly.*

Index Terms--- *Secured Network Mobility, Mobile Virtual Private Network (MVPN), Session Initiation Protocol (SIP), Performance Analysis*

I. INTRODUCTION

THE goal of the Network Mobility study is to describe the operations of the Internet for supporting Mobile Network. Network Mobility, the movement of a complete network that changes its point of attachment to the fixed infrastructure and maintains the sessions of every device of the network.

The Network Mobility comprises of Home Network and Foreign Network. The Home Network remains fixed and it is the intranet. The Foreign Network moves from one IP subnet to another and it is the internet.

P. Thamaraikannan, Master of Engineering (Pursuing), Dept. of Computer Science & Engineering, Apollo Priyadarshanam Institute of Technology, Chennai. India. E-mail:pkannan1984@gmail.com

P. Vijayaragavan, M. Tech., Assistant Professor, (Head of the Department), Dept. of Computer Science & Engineering, Apollo Priyadarshanam Institute of Technology, Chennai. India.

A. List of Acronyms

ALG	Application Level Gateway	RTCP	RTP Control Protocol
AVP	Attribute Value Pair	RTP	Real-time Transport Protocol
CN	Correspondent Node	SA	Security Association
CoA	Care of Address	SDP	Session Description Protocol
HA	Home Agent	SeNEMO	Secure NEMO
IKE	Internet Key Exchange	SIP	Session Initiation Protocol
i-HA	internal HA	SIP-NVG	SIP NEMO VPN Gateway
i-MIP	internal MIP	SRTP	Secure Real-time Transport Protocol
MAA	Multimedia-Auth-Answer	TEK	Traffic Encryption Key
MAR	Multimedia-Auth-Request	TGK	TEK Generation Key
MIDCOM	Middlebox Communication	UAA	User-Authorization-Answer
MIKEY	Multimedia Internet Keying	UAR	User-Authorization-Request
MIP	Mobile IP	VPN	Virtual Private Network
MN	Mobile Node	VPN-TIA	VPN Tunnel Inner Address
MR	Mobile Router	x-HA	external HA
NEMO	Network Mobility	x-MIP	external MIP
PAN	Personal Area Network		

B. Personal Mobility

Personal mobility allows a human being to access or to be accessed by the network independently of where the access point and terminal used are located in the network and maintaining all services contained in the personal subscription. An example can be a person who wants to be contacted on his stationary PC in the office during the working hours and by an IP-phone at home the rest of the day.

C. Terminal Mobility

Terminal mobility permits a terminal to change location while maintaining all the services. Terminal mobility can be provided at different layers and thus, different approaches exist. Mobile IP is an example of how terminal mobility can be achieved on the network layer.

D. Application Mobility

Application mobility allows a software process to be relocated from one machine to another or even moved between machines while processing.

E. Session Mobility

Session mobility is defined as an added feature to those mentioned above. This mobility is ensuring that active sessions are not disrupted while terminals, persons or applications are moving or being relocated (However, sessions may be brought to a well-defined halt state in order to be resumed later). One example of session mobility is call transfer, e.g. a user can move from one terminal with multimedia presentation capabilities to one with voice-only capabilities or vice-versa.

F. Role Mobility

Role mobility is a new type of mobility arising recently. As a member of the society, each individual has usually multiple roles, e.g. employee of a company, head of a family, etc. Furthermore, an individual may have several job positions in different companies and hence different roles. For each role,

ISBN 978-93-82338-61-1 | © 2013 Bonfring

there is defined a set of services with distinct preferences, rights and limitations. Role mobility aims to assist the user to move from one role to another easily and smoothly.

G. Overview of the Project

The IETF Network Mobility (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. In this paper, we consider how to provide Virtual Private Network (VPN) services in Network Mobility. Security has become a critical issue for today's Internet. VPN has been developed to secure user's communication between untrusted external networks (internet) and the protected private internal network (intranet). VPN services over Network Mobility can be used in a variety of applications so a mobile network can access to its intranet in a secure way.

Network Mobility does not support VPN, so a new architecture and protocols to support VPN in Network Mobility is developed and it is called Secure Network Mobility. The proposed Secure Network Mobility is based on Session Initiation Protocol (SIP), is specifically designed for real-time applications over mobile VPN for group mobility. It allows an entire network to move from one location to another location while still maintaining its local nodes ongoing sessions. Secure Network Mobility maintains a secure sessions during network handoff and node handoff.

In our proposed Secure Network Mobility, a URI list is used to inform SIP Proxy Server instead of sending the information for each MN individually. Thus signaling cost is reduced. Various IETF protocols have been adopted in Secure Network Mobility. The SIP Proxy Server and the Diameter Server are responsible for the authentication and authorization. The ALG accepts the commands from SIP Proxy Server to process the security information for data transmission by following the MIDCOM architecture. For key management, we adopt MIKEY to exchange the shared TGK that is used to protect data transport.

II. Related Work

The IETF MVPN cannot be applied to NEMO because it does not consider the mobility of a group of mobile devices. Besides, the IETF solution, which is based on IPsec and MIPv4 [3], will incur long handoff latency and end-to-end latency [4]. The three tunnels (one IPsec tunnel and two MIP tunnels) increase around 100 bytes for the packet length, which is relatively five times of the length of a G.7291 real time packet [5]. 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, where to put the x-HA and how to trust the x-HA are critical issues. To better support real-time applications, a SIP-based mobile VPN has also been proposed [6]. However, it considers the VPN for the movement of a single node only.

III. Existing System

Route Optimization, a mechanism that optimizes the transmission of packets or mechanism to enable packets to directly reach the mobile network. The Route Optimization schemes are classified based on the basic approach and they are, a). Delegation approach b). Hierarchical approach c).Source routing approach d). BGP-assisted approach. The protocol overhead includes header overhead, amount of signaling and memory requirements[1].

NEMO provides mobility solution based on Mobile Router concept. Mobile Router maintains session continuity between the Mobile Network Nodes (MNN) and the Correspondent Node (CN), irrespective of the Mobile Router's change of point of attachment. Route Optimization (RO) and it presents highlights of different scenarios of the NEMO RO and analysis of the corresponding proposed solutions[2].

CRYptographic Prefixes for Route Optimization in NEMO". As currently defined, NEMO Basic Support protocol lacks of Route Optimization support which is an essential requirement for its adaptation as part of the next generation ATN. In CRYPTON, the Crypto Prefixes are used to protect the establishment of the bindings on the Correspondent Nodes for the whole Mobile Network Prefix[3].

Network Mobility (NEMO) extension to MIPV6 has to be considered, but this protocol does not yet provide any Route Optimization procedure, although many proposals do exist. This approach is based on certificates that should allow reducing signaling overhead and handover delay while providing a higher level of security [4].

NEMO is an extension protocol to mobile IPV6 in providing seamless connection to every node in the network. By using the mobile router, mobility support is provided to each fix or mobile node in the network even though there is a change in the network topology in a sense that the mobile router changes the point of attachment to the network. In this paper, we will discuss and provide route optimization by adapting Ad-hoc On Demand (AODV) routing protocol into NEMO environment [5].

The DRO scheme that incorporates the domain-based network architecture and the operations of ad hoc routing protocols to perform the route optimization. The packet transmission delay and the handoff latency should be significantly reduced [6].

A. Issues in the Existing Systems

The literature survey presented above gives the overview of some new systems and novel approaches in the field of Network Mobility. In this survey, the security, signaling overhead and route optimization are dealt with. Some of the issues encountered are listed below:

- Security is a critical issue.
- Performance is not ensured in Network Mobility.
- Transmission delay and hand off latency are high in Network Mobility.
- Signaling cost is high in NEMO.

ISBN 978-93-82338-61-1 | © 2013 Bonfring

IV. PROPOSED SYSTEM

Mobile Virtual Private Network has been developed to secure mobile user's communication between untrusted external networks and the protected private internal network, but NEMO does not support VPN. Secure Network Mobility, the architecture and protocols are proposed to support VPN in NEMO and it is based on Session Initiation Protocol (SIP). SIP keeps ongoing sessions, maintains session continuity and reduces transmission delay. The SeNEMO is designed for real time applications. It allows an entire network to move from one location to another and still maintains session continuity. The security and the performance is analyzed using analytical and mathematical models. Extensive simulations have also been conducted to validate the analysis.

A. System Architecture

System architecture is the conceptual model that defines the structure and behavior of the system. The system architecture for the proposed system Secure Network Mobility architecture is given in Figure 1.0

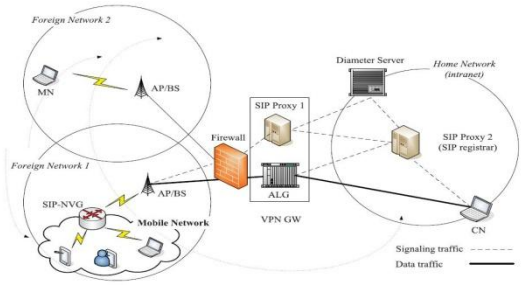

Fig.1: System Architecture

B. Signaling

SIP is an application-layer signaling protocol. It is used to create, modify, and terminate sessions in the proposed SeNEMO. SIP has defined its own security and authentication schemes.

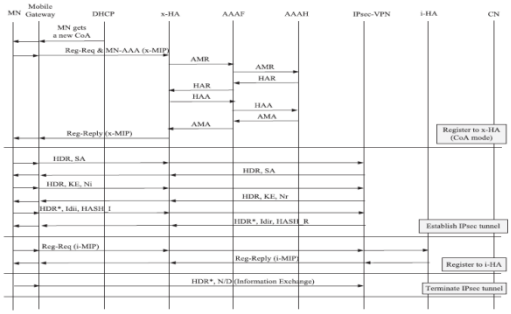

Fig. 2: Signaling Flows of IETF MVPN

In our proposed SeNEMO, we use them to authenticate and identify the mobile users. SIP also supports user mobility and terminal mobility. The terminal mobility is achieved by sending new INVITE (re-INVITE) to the CN by using the same call ID as that in the original session. After receiving the re-INVITE, the CN will redirect future traffic to the MN's new location.

C. Secure Transport

SRTP defines a framework to provide encryption and integrity for Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) streams. SRTP also provides replay protection based on the RTP sequence number and the index number of RTCP. The predefined cryptographic transformations provide low computational cost and limited packet expansion so bandwidth can be used more economically than IPsec. It is also independent of the underlying transport networks.

D. Key Management

MIKEY is a key management protocol developed for multimedia real-time applications running over RTP/ SRTP. Comparing with IKE which is widely used as key management protocol for unicast, MIKEY is designed. SeNEMO protocol stacks for control plane when the mobile network is in internet and CN is within intranet. MIKEY can fulfill the requirements of different environments. 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. TGK is an upper-level key, which is shared within an interactive group. It is used to derive TEK for each cryptographic session. The Data SA is used as input of security transport protocol, such as SRTP.

E. Application Authenticated Authorized (AAA)

Based on the Diameter base protocol, 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. The authentication is done by Diameter server rather than by delegating to a SIP server.

F. Security Vulnerabilities in SeNEMO.

The proposed SeNEMO is designed based on SIP, the security problems in SeNEMO might be inherited from SIP. The security problems in SIP have been widely studied. Message flows when mobile network roams from home network to foreign network. SIP authentication: Like other common deployment of SIP, the proposed SeNEMO uses a challenge-response based protocol to verify users. 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 SeNEMO, the transport of SIP messages can be easily extended to incorporate Transport Layer Security (TLS) so the transmission of SIP messages can be protected.

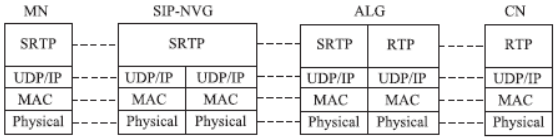

Fig.3: SeNEMO Protocol Stacks for User Plane when the Mobile Network is in Internet and CN is within Intranet

Denial of service (DoS): Protecting against DoS attacks is inherently difficult on IP networks, especially for mobile networks such as MIP. Similarly, the open architecture of the

ISBN 978-93-82338-61-1 | © 2013 Bonfring

Internet may expose any SIP network element, such as Registrar server or Proxy server, to DoS attacks.

However, in the proposed SeNEMO, SIP Proxy2/Registrar and Diameter server are located inside the intranet. Therefore, they are much less vulnerable to DoS attacks. Besides, the ALG can block all the messages coming from unknown nodes unless the resources are reserved for legitimate users by SIP Proxy 2. Although SIP Proxy 1 which is on the border may be subject to DoS attacks, a large portion of the effects can be reduced by proper server design and efficient implementation by adequate hardware.

SIP application-level attack: An attacker may send fake BYE, CANCEL, or re-INVITE to terminate a Session, cancel an invitation, or redirect a call**.** In the SeNEMO, such attacks can be prevented by the proposed SIP authentication mechanism and Diameter SIP Application.

G. Media Security

The proposed SeNEMO uses MIKEY to transport Data SA and SRTP to secure real-time streaming. Therefore, MNs can securely communicate with CNs even if staying outside the intranet. Please note SRTP provides confidentiality, integrity, and replay protection only for the application data. The UDP and IP headers are not protected as that in IPsec. The comparison of security vulnerabilities in SeNEMO and IETF MVPN is summarized.

V. MODULAR STRUCTURE

The proposed system consists of the following modules,

A. Movement of MN in Home Network

When the Mobile Node moves into the Home Network and wants to connect to the Correspondent Node in the Home Network, first the MN registers to the SIP-NVG.

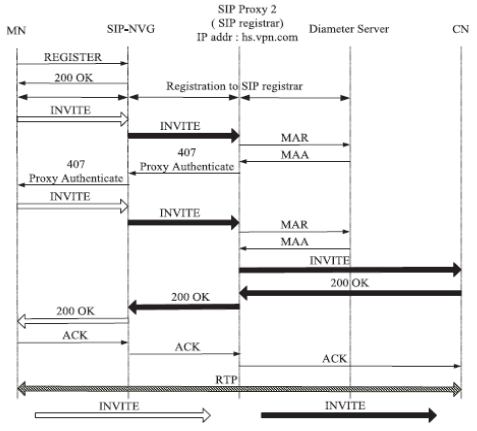

Fig. 4: Message Flows and Translation of INVITE when MN Moves to a Mobile Network which is located inside Home Network

The SIP-NVG routes the SIP messages to the SIP Proxy 2, which is a SIP Registrar through the Diameter Server. The SIP Proxy 2 sends the request message to the CN and then the CN acknowledges it. And finally the MN and CN communicate directly.

B. Movement of MN in Foreign Network

When the MN moves out of the intranet, it first requires a new CoA and it gets it from the SIP-NVG. The SIP-NVG routes the SIP messages to the SIP Proxy1. The SIP Proxy 1, which authenticates the incoming SIP messages through the Diameter Server and routes SIP messages to SIP Proxy 2. The SIP Proxy 2 transmits that message to the ALG, which replaces the header with a new one. And finally the MN communicates to the CN through the ALG.

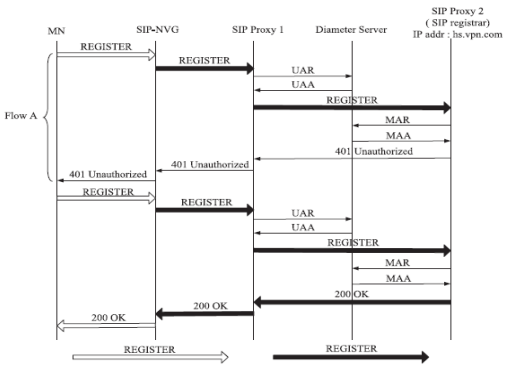

Fig. 5: Register when Mobile Network resides in Foreign Network

C. Security Analysis

The qualitative analysis of security vulnerabilities in the proposed Secure Network Mobility,

- SIP authentication
- Denial of service(DOS)
- SIP parser attack
- SIP application-level attack
- Media security

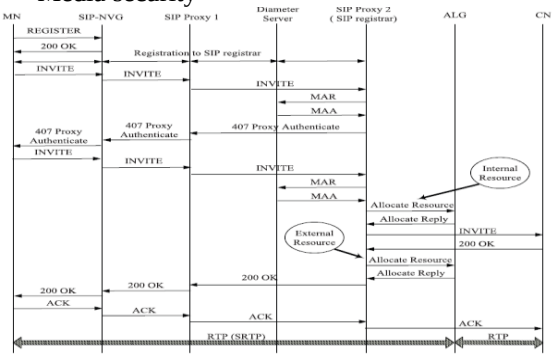

Fig. 6: Message Flows when MN moves to a Mobile Network which is Located inside a Foreign Network for Security Functions

D. Performance Analysis

In order to support secure communication in VPN, signaling messages carrying security information are sent to maintain session continuity during handoff in SeNEMO.

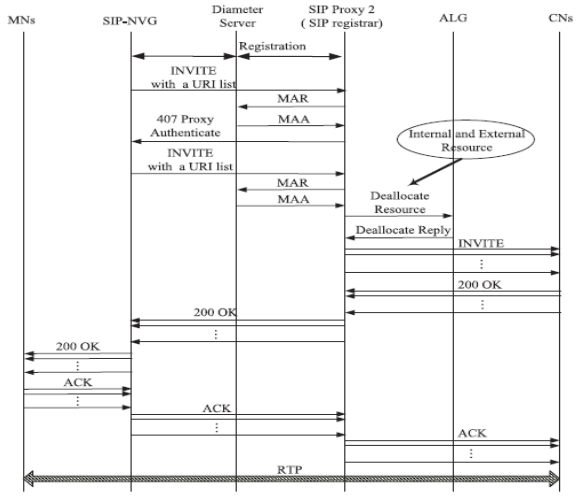

Fig. 7: Performance in Mobile Network Roams from a Foreign Network back to Home Network

The signaling cost of the proposed SeNEMO is analyzed. 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.

VI. Conclusion

The design and analysis of SeNEMO, which integrates NEMO and VPN. The proposed SeNEMO is based on SIP, which makes it particularly suitable for real-time services. Although SIPased mobility management is easy to support route optimization, by adopting SIP into NEMO, it may increase signaling cost during handoff due to sending many re-INVITE messages for ongoing sessions. In our proposed SeNEMO, a URI list is used to inform SIP Proxy Server instead of sending the information for each MN individually. Thus, signaling cost is reduced. Various IETF protocols have been adopted in SeNEMO. The SIP Proxy Server and Diameter Server are responsible for authentication and authorization.

The Diameter Server exchanges the TGK with the MN on behalf of CN. The SIP Proxy Server will transmit TGK to ALG. The ALG is responsible for switching and relaying the protected and unprotected data. Therefore, unauthorized data cannot pass through ALG into the intranet. In addition to analyzing the security vulnerabilities, we also propose analytical models to compare the performance of the proposed SeNEMO with IETF MVPN.

Acknowledgment

I must thank, first and foremost, my Project Guide Mr. P. Vijayaragavan., M. Tech., Assistant Professor, Department ofcomputer science and engineering, without whose guidance and patience, this dissertation would not be possible. I wish torecord my thanks to project panel members, Professors of the Department of Computer Science and Engineering for their consistent encouragement and ideas.

References

[1] Abu Zafar M. Shahriar and Mohammed Atiquzzaman (2012) 'Route Optimization in Network Mobility: Solutions, Classifications, Comparison and Future Research Directions', Proc. Communications, Vol. 12 No.1 pp.24-38.

[2] Ahmed A. Mosa and Aisha Hassan (2011) 'Evaluation of NEMO-Based Approaches for Route Optimization', Proc. Conf. Mechatronics, pp.1-7.

[3] Ana Kukec and Marcelo Bagnulo (2010) 'CRYPTRON: CRYptographic Prefixes for Route Optimization in NEMO', Proc. Conf. Communications, pp.1-5.

[4] Christian Bauer and Wessling (2010) 'Network Mobility Route Optimization with Certificate-based Authentication', Proc. Conf. Ubiquitous and Future Networks, pp.189-194.

[5] Seong - Yee Phang and HoonJae Lee (2009) 'Route Optimization for NEMO Based on AODV', Proc. Conf. Advanced Communication Technology, Vol. 2 pp.1396-1400.

[6] Ming-Chin Chuang and JengFarn Lee (2010) 'DRO: Domain-Based Route Optimization scheme for nested mobile networks', Proc. Conf. Wireless Communications and Networking, pp.1-6.