2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

Secured MPLS-based Mobile IP using the Private IP Address

Sriborrirux Wiroon, Jeong-Beom Kim, Rhe yun-jung and Tai-Yun Kim

Computer Science and Engineering, Korea University

{wiroon, qston, genuine, tykim}@netlab.korea.ac.kr

Abstract

The number of connected computers in the Internet, which has reached a state in which its address space is becoming insufficient, is exponentially increased. Also nowadays modern Laptops and Mobile terminal are being used more and more. As known, the number of available IPv4 address is limited and many organizations have limited budget to use the global address. So the way to overcome such problems is using private addresses in their networks. In addition, the use of private address makes the system more secure. Moreover, we have considered about supporting of the scalability of data forwarding processes of nodes in their network especially Mobile IP data communication. Thus, we propose the integration of MPLS and Mobile IP network. Also we propose the security services of a constrained LSP for the MPLS payloads.

1. Introduction

Currently, new technologies and protocols have been developed to provide to mobile users the services that already exist for non-mobile users. Mobile IP protocol [1], one of these technologies, enables a node to change its point of attachment to an Internet. The protocol uses two mobility management elements called mobility agents to help mobile nodes (MN). A home agent (HA) in the home network of MNs provides support for movement. A foreign agent (FA) helps MNs in foreign networks when MN visits it by advertising available Mobile IP service and by act as a router for MNs. A user who wants to send packets to the Mobile Host is called a Correspondent Node (CN). The three different activities of Mobile IP's operation are the agent advertisement process, the registration process, and tunneling process. They are significant processes in order of the Mobile IP protocol to be scalable of systems, which consists of large numbers of mobile hosts.

Private IP address, as proposed in 1991 [2], was introduced to reduce the address space shortage. These addresses may not be globally unique as several organizations can use such addresses inside their own networks with coordinating the used addresses with other organizations. To make the mobility management feasible for all mobile nodes protocols need to support private addresses. Moreover, the HAs, which are located at the edge between the global network and private network, need the mechanism for communication between a private and a global address. The mentioned mechanism is using the Network Address Translator (NAT) [3]. The traditional NAT works by translating the address fields of IP packet headers. A router translates the private addresses to global addresses from a spool of available addresses.

MultiProtocol Label Switching (MPLS) [4] is a new technology that will be used by many future networks. MPLS forwards data using the label attached to each data packet between Label-Switched Routers (LSR) along with Label-Switched Paths (LSP) as figure shown.

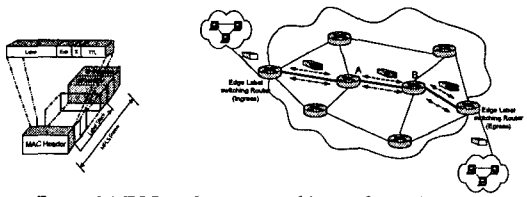


Figure 1 MPLS Architecture and MPLS frame format

When an IP packet enters an LSP, the ingress router examines the packet and assigns it a label based on its destination, placing the label in the packet's header. The label transforms the packet from one that is forwarded based on its IP routing information to one that is forwarded based on information associated with the label.

In this paper, we consider three main issues; e.g. the limitation of IPv4 addresses, the scalability of Mobile IP data forwarding process and the security services of the MPLS payload and LSP. So we propose to assign a private IP address to MN to solve the

problem called "Address Starvation Problem". Also in order to improve the scalability of Mobile IP data forwarding process, we agree to integrate of Mobile IP and the MPLS by leveraging on the features of MPLS, which are fast switching, small state maintenance, and high scalability. Since the traditional MPLS itself does not provide encryption, integrity, or authentication services. If MPLS core is not configured with the necessary security measures, Mobile IP network could be exposed to some forms of attack. So we propose the extension of LDP message to transport the key along with a constrained LSP to make negotiation of security on MPLS-based Mobile IP network.

2. Related works

In [5], they proposed an approaches to realize Mobile IP protocol by assigning a private IP address to mobile node. They presented installation of NAT function within mobility agents. Also in order a CN to make a call to a MN, DNS procedure and NAT function are used in HA.

About Integration of MPLS and Mobile IP from [6], it showed that the integrated scheme can significantly improve the scalability and performance of Mobile IP. As experiments, they showed that the Packet Switching at MPLS Layer is much faster than conventional IP forwarding at IP Layer. Moreover, the transmission delay and packet-processing overhead are reduced obviously as seen from their experiments.

And [7] has proposed to secure MPLS payloads along the LSP. Also [8] presented CR-LDP as the extension of Label Distribution Protocol (LDP) to set up a constrained path.

The rest of this paper is organized as follows: in section 3, we propose the integration of MPLS and Mobile IP using Private IP address including NAT and DNS server. Next, we also propose the modification of LDP message to transport IKE for the security service issue in section 4. After that, section 5 describe the detail procedures for MPLS-based Mobile IP with Private IP addresses. Finally, the summary is the rest of this paper.

3. The integration of MPLS and Mobile IP using Private IP address including NAT and DNS server.

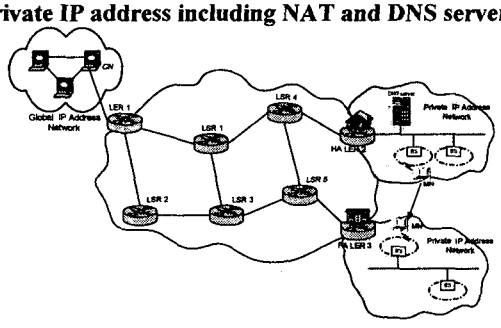


Figure 1 MPLS-based MIP Network using Private IP Address

In this paper, we propose the functions of HA and FA similar to [5], as router that are located at the border of closed network with Private IP Addresses, and they provide the NAT function and the coordination between DNS procedure and mobile IP/NAT procedure in case of making a call from CN to MN.

We introduce the integration of Mobile IP using Private IP Address and MPLS scheme, which can improve the scalability and high-speed IP forwarding of Mobile IP data forwarding process by leveraging on the features of MPLS without using the IP-in-IP tunneling [9].

4. Modification of LDP Frame to transport IKE

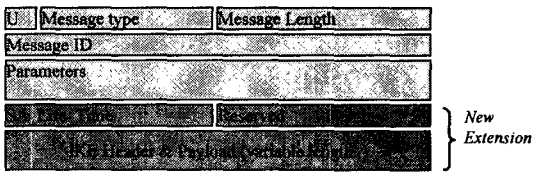
Use of the IPSec ESP protocol to provide parts or all traffic over the MPLS core, If an attacker is able to sniff traffic on the core, with IPSec attacker will be able to see only the site from coming and going to. Also in case of using the IPSec AH protocol particularly the endpoints (LERs), the attacker can not introduce another LSR in the MPLS-based MIP, save a packet flow, and replay it later called Replay Detection, even if the MIP's MPLS core is not fully secured. Moreover, the integrity of the traffic-Packets cannot be changed on their way through the core without the change being noticed. Bogus packets cannot be introduced from the core. Ensuring Location Privacy requires the use of IPSec ESP in tunnel mode for the mobile node to correspondent node traffic.

Use of IPSec running over MPLS cloud is essential where preventing session stealing, eavesdropping and DoS attacks on physically insecure shared network media (e.g. Ethernet or wireless links) is a concern.

As [7], they proposed the establishment of SA between end-to-end to define the algorithms for encryption, authentication, hash and key exchange for protecting a LSP. The Internet Key Exchange (IKE) defines the messaging protocol used to establish required SA for key distribution. In this paper, we decide to use CR-LDP to set up a constrained LSP. So the ability to perform IKE over CR-LDP in order to avoid the need of a separate IP control channel. Using LDP extension to carry IKE message between LSRs in order to each LSR exchange the SA negotiation to each other, we propose the new extension of LDP message in order to enable end-to-end authentication between LSRs as explained below.

Secure LDP messages Format

All LDP messages have the following format.



If message type is 0x500 (*new proposed message type*), it means this payload is ISAKMP(a protocol to establish a framework authentication and key exchange).

SA_Life_Time:

Specifies the number of seconds before the SA will expire.

5. Detail Procedures

- *Agent Advertisement/Discovery and Registration Procedure*

Figure 2 below shows the procedure that a MN registers its location to HA when it moves to a visited network through a constrained LSP in MPLS infrastructure.

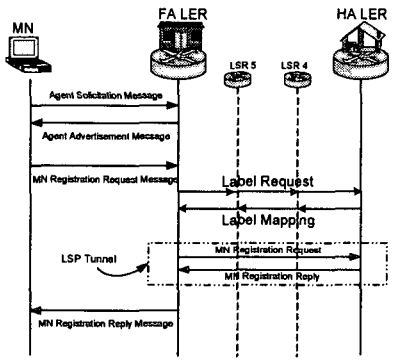


Figure 2 Agent Advertisement and Registration Procedure

MN will send Agent Solicitation message to ask for an Agent Advertisement message sent by FA. The message obtains the IP address of FA and a related COA. When MN detects Agent Advertisement message, then it sends a Registration Request message to FA. Before FA relay a Registration Request message to HA, a LSP should be established first. After the establishment of LSP is finished, FA relays a Registration Request message to HA (the source and destination addresses are the global IP addresses of FA and HA respectively).

After that, HA receives a Registration Request message sent from FA and responds a Registration Reply message to FA (the source and destination addresses are the global IP addresses of HA and FA respectively).

- *MN initiated Communication Procedure*

Figure 3 below shows the procedure that a MN using private IP address want to communicate with CN using global IP address in the global IP network.

First, MN sends data packet to FA which the source and destination IP address of this data packet is MN's private IP address and CN's global IP address respectively. FA checks whether a global IP address is already assigned to MN. If not, FA asks HA (with NAT function) for assigning global IP address to MN by sending an Address Assign Request message containing MN's private IP address. Before sending this message, we propose to establish LSP to protect it from attackers. When HA selects one of the global IP addresses and assigns it to MN. It maintains the mapping among MN's private IP address, assigned MN's global IP address, its lifetime and FA's global IP address [*IPpri(MN), IPglo(MN), TTL, IPglo(FA)*]. HA replies an Address Assign Reply message containing MN's global IP address and its lifetime to FA in order FA to maintain the mapping among MN's private IP address, MN's global IP address and its lifetime [*IPpri(MN), IPglo(MN), TTL*]. To make to completing tunnel between MN and CN, there is the set up a constrained LSP between them. As we described before, the path will be authenticated by exchanging the key between them. Thus, data packets are protected during transmit along with these LSPs.

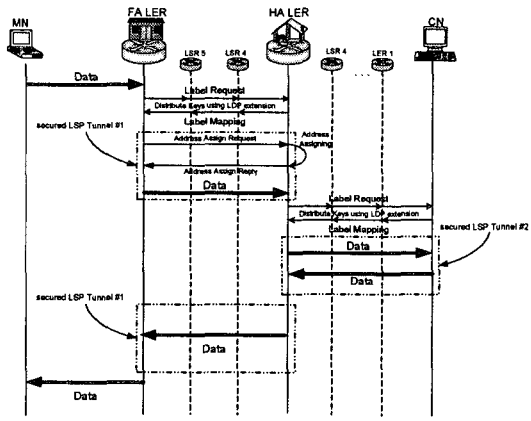


Figure 3 MN initiated Communication Procedure

CN initiated Communication Procedure

Figure 4 below shows the procedure that a CN using global IP address want to make a call to MN using private IP address.

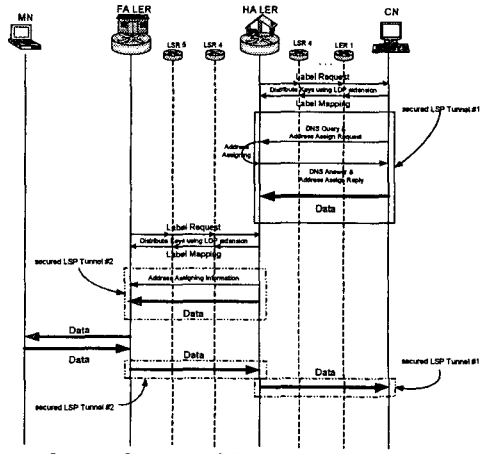


Figure 4 CN initiated Communication Procedure

Establishing the LSP and exchanging the key to each other already, then CN sends a DNS query and Address Assign Request message containing Fully Qualified Domain Name (FQDN) of MN to HA. The DNS server maintains the mapping of FQDN and MN's private IP address. When HA receives MN's private IP address from DNS server, it selects one of the global IP addresses to assign it to MN. After that, HA maintains the mapping among MN's private IP address, MN's global IP address, its lifetime and FA's global IP address *[IPpri(MN), IPglo(MN), TTL, IPglo(FA)]*.

HA sends an Address Assign Reply message containing MN's global IP address and its lifetime to the DNS server. CN knows the global IP address of MN from a DNS Answer message sent from DNS server through HA. And HA have to let FA know the mapping between MN's private IP address and MN's global IP address as well by sending Address Assign Information message to FA after setting up a LSP already.

Some problems may occur e.g. Private Address Collision due to multiple MNs with the same private IP address assigned by different home networks exist in one visited network simultaneously and management of lifetime. For the first problem, we agree with [5] by letting FA check the source MAC address of that packet. Also next problem occurs due to a global IP address assignment or DNS cache consistent with global IP address assignment by HA, as proposed in [5].

Summary

In this paper, we have proposed the integration of Mobile IP using Private IP Address and MPLS scheme. Since using the features of MPLS, it can improve the scalability and high-speed IP forwarding of the Mobile IP data forwarding process without using the IP-in-IP tunneling. Moreover, we have proposed the security services for data packets (MPLS payload) along with a LSP using CR-LDP to transport IKE between LERs.

References

1. C. Perkins, Editor, "IP Mobility Support", RFC 2002, October 1996.

2. Y. Rekhter, et al., "Address Allocation for Private Internet ", RFC 1597, March 1994.

3. K. Egevang and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, May 1994.

4. Rosen, E., Viswanathan, A., and R. Callon, "MultiProtocol Label Switching Architecture", RFC 3031, January 2001.

5. Toshihiko Kato, Akira Idoue and Hidetoshi Yokota, "Mobile IP Using Private IP Address", March 2001.

6. Ren Z., et al., "Integration of Mobile IP and MPLS", <draft-zhong-mobile-ip-mpls-01.txt>, July 2000.

7. Senevirathne Tissa, and Paridaens Olivier, " Secure MPLS - Encryption and Authentication of MPLS payloads", <draft-tsenevir-smpls-01.txt>, February 2001.

8. Jun Kyun Choi, et al., "Extension of LDP for Mobile IP Service through the MPLS Network", <draft-choi-mobileip-ldpext-02.txt>, August 2001.

9. W. Simpson, "IP in IP tunneling", RFC 1853, October 1995.