TraSH: A Transport Layer Seamless Handover for Mobile Networks

Shaojian Fu[1], *Mohammed Atiquzzaman*[1], *Liran Ma*[1], *William Ivancic*[2], *Yong-Jin Lee*[1], *Justin S. Jones*[1], *Song Lu*[1]
[1]Telecommunications and Networks Research Lab, School of Computer Science,
University of Oklahoma, Norman, OK 73019-6151, USA.
[2]Satellite Networks & Architectures Branch, NASA Glenn Research Center
21000 Brookpark Rd. MS 54-8, Cleveland, OH 44135.

Technical Report: OU-TNRL-04-100
January 2004

***Abstract*— The Internet Engineering Task Force has developed Mobile IP to handle mobility of Internet hosts at the network layer. Mobile IP, however, suffers from a number of drawbacks such as high handover latency, packet loss, and conflict with network security solutions. In this paper, we describe TraSH, a new Transport Layer Seamless Handover solution to mobility. TraSH utilizes multi-homing to achieve a seamless handover of a mobile host, and is designed to solve many of the drawbacks of Mobile IP. Various aspects, such as handover, signalling, location management, data transfer, and security considerations of TraSH are discussed. The Stream Control Transmission Protocol (SCTP), with built-in multi-homing capability, is used to illustrate the concepts of TraSH.**

I. Introduction

Mobile IP (MIP) [1] is the standard proposed by IETF to handle mobility of Internet hosts for mobile data communication. For example, it enables a TCP connection to remain alive and receive packets when a mobile host moves from one point of attachment to another. Mobile IP is based on the concept of Home Agent (HA) and Foreign Agent (FA) for routing of packets from one point of attachment to the next. During the handover from the HA to the FA, a mobile host (MH) will need to register with the FA, wait for the allocation of channels, and update its location in the HA database.

While MIP is a widely accepted concept in both research and industry, several problems exist when using MIP in a mobile computing environment. The most important issues of MIP identified to date include:

- High handover latency [2]: A MH needs to complete the following three steps before it can receive forwarded data from the previous point of attachment: (i) discovering the new Care of Address (CoA), (ii) registering the new CoA with the HA, and (iii) forwarding packets from the HA to the current CoA.
- High packet loss rate [3], [4]: During the HA registration period, some or all of the packets destined to the MH's old CoA will be lost since the old point of attachment can not communicate with the MH during this period, nor does it know the new point of attachment of the MH.
- Inefficient routing [2]: In base MIP, large amount of data is routed to the HA, and then tunnelled to the MH. This wastes network resources and requires high processing power at mobile agents (HA and FA). This may give rise to scalability issues as the number of MHs managed by a HA increases. Moreover, the failure of a single HA may prevent a large number of mobile users from receiving forwarded packets from the HA unless a backup scheme like automatic HA discovery is used.
- Conflict with network security solutions [2]: Base MIP does not cooperate well when the HA is behind a firewall and the MH is outside the firewall, unless firewall transversal solution [5] is used. Moreover, base MIP has difficulty in the presence of a foreign network implementing ingress filtering, unless reverse tunnelling, where the HA's IP address is used as the exit point of the tunnel, is used to send data from the MH.

The research reported in this paper was funded by NASA Grant NAG3-2922

A. Recent research on Mobile IP

Research efforts in Mobile IP can be generally classified into two categories: reducing handover latency and packet loss. Hierarchical IP [6], Hawaii [7], Cellular IP [8] use Hierarchical foreign agent structure to reduce the frequency and latency of binding updates by handling most of the handovers locally. A hierarchical FA structure also reduces the possibility that packets are directed to an outdated FA by multiple tunnelling process, thus reducing the packet loss rate. Low latency handoffs in Mobile IPv4 [4] use pre-registrations and post-registrations by utilizing link layer event triggers to reduce the handover latency. Optimized smooth handoff [9] not only uses the hierarchical FA structure, but also makes the previously visited FA buffer to forward packets to MH's new location. To facilitate packet rerouting after handover and reduce packet losses, Jung et.al. [10] introduces location database that maintains the time delay between the MH and the crossover node. Mobile Routing Table (MRT) has been introduced at the home and foreign agents in [11], and a packet forwarding scheme similar to [9] is also used between FAs to reduce packet losses during handover. A reliable mobile multicast protocol (RMMP) proposed in [12] uses multicast

to route the missing packets to adjacent subnets to ensure low packet loss rate resulting from MH roaming.

To eliminate the triangular routing problem, Route Optimization (RO), an optional feature in Mobile IPv4, allows a Correspondent Node (CN) to send packets directly to the MH's new COA address. RO is built in as an integral part of Mobile IPv6 [13]. In Mobile IPv6, the concept of foreign agent has been removed since the available IP address space is large and the MH can easily get a co-located COA (CCOA) address. As a result, the MH itself acts as the exit point of the packet tunnel. Like the Hierarchical IP [6] in MIPv4, Hierarchical MIPv6 mobility management [14] also introduces a hierarchy of mobile agents to reduce the registration latency and the possibility of an outdated CCOA address.

B. Motivation of TraSH

As the percentage of real-time traffic over wireless networks keeps growing, the deficiencies of the network layer based Mobile IP in terms of high latency and packet loss becomes more obvious. The question that naturally arises is: Can we find an alternative approach to network layer based solution for mobility support? Since most of the applications in the Internet are end-to-end, a transport layer mobility solution would be a natural candidate for an alternative approach.

A new transport protocol, called Stream Control Transmission Protocol (SCTP), was proposed by IETF in October 2000.The design of SCTP absorbed many of the strengths of TCPthat led to its success during the explosive growth of the Internet. Moreover, SCTP incorporated several new features that are not available in TCP. Due to its new attractive features, SCTP has recently received much attention from the research community, and has become one of the hot topics in networking technology [15], [16], [17].

Multi-homing is one of the most prominent features of SCTP. The built-in multi-homing support in SCTP was initially designed to exploit network redundancy to meet the requirements of high-availability applications (such as communication between SS7 signalling points). But this feature can also be very useful in mobile computing environments. As pointed out in Sec. I, with only one COA address in MIP, the MH cannot communicate with the old mobile agent while the MH is registering with the new mobile agent. This restriction gives rise to *high handover latency* and *high packet losses*. Even if the various proposed improvements [6]-[14] for MIP are used, this fundamental restriction can not be overcome, since different MIP extensions still use only one interface for communication.

The *objective* of this paper is to propose a new scheme for supporting mobility called Transport Layer Seamless Handover (TraSH) by utilizing SCTP's multi-homing feature. Similar in principle to a number of current efforts [18], [19], [20], the basic idea of TraSH is to exploit multi-homing to keep the old path alive while setting up the new path, thus achieving a seamless handover between adjacent subnets. Although we illustrate TraSH using SCTP, it is important to note that TraSH can cooperate with normal IPv4 or IPv6 infrastructure without the support of Mobile IP.

C. Contributions of current research

The contributions of our paper can be outlined as follows:

- Propose and develop Transport Layer based Seamless Handover (TraSH) that is expected to solve several problems faced by MIP. Here "seamless" means low latency and low packet loss.
- Illustrate the handover procedure and location management in TraSH and compare them with MIP.
- Compare the data transfer paths of TraSH and MIP.
- Discuss the security considerations of the new scheme.

D. Paper structure

The rest of this paper is structured as follows: Sec. II gives a brief introduction to SCTP's multi-homing feature, Sec. III outlines the handover signalling procedures in TraSH, Sec. IV discusses location management method that can be used with TraSH and the data transfer path used by TraSH after the handover. Performance comparison between TraSH and MIP is provided in Sec. V. Sec. VI discusses the security considerations of TraSH. Finally, concluding remarks are presented in Sec. VII.

II. A Brief Introduction to SCTP Multi-Homing

Multi-homing allows an association between two end points to span across multiple IP addresses or network interface cards. An example of SCTP multi-homing is shown in Fig. 1, where the two end points are connected through two wireless access networks. The correspondent node (CN) is single-homed, while the Mobile Host (MH) is multi-homed. The MH can use one or two interface cards as long as the two IP addresses can be bound into the association. One of the MH's IP addresses is designated as the primary destination address for the transmission of data by the CN, while the other one can be used as a backup in the case of failure of the primary address, or when the upper layer application at the CN explicitly requests the use of the backup address.

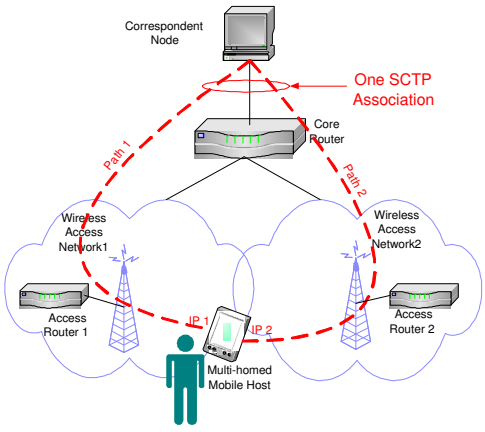


Fig. 1. An SCTP association with multi-homed mobile host.

Retransmission of lost packets can also be performed over the backup address. SCTP's built-in support for multi-homed endpoints is especially useful in environments that require

high-availability applications, such as SS7 signaling transport. A multi-homed SCTP association can speedup the recovery from link failures without interrupting the data transfer [21].

III. HANDOVER SIGNALLING IN TraSH

We assume that the direction of traffic flow is from the CN to MH, which corresponds to services like file downloading or web browsing by mobile users. In this section, we outline TraSHś signalling procedure during the handover process. The complete handover procedure can be divided into five parts which are described below. The main idea of TraSH is to exploit multi-homing to keep the old data path alive until the new data path is ready to take over the data transfer, thus achieve a low latency, low loss handover between adjacent subnets.

A. STEP 1: Obtain new IP address

Referring to Fig. 1, the handover preparation procedure begins when the MH moves into the overlapping radio coverage area of two adjacent subnets. Once the MH receives the router advertisement from the new access router (AR2), it should initiate the procedure of obtaining a new IP address (IP2 in Fig. 1). This can be accomplished through several methods: DHCP, DHCPv6, or IPv6 Stateless Address Autoconfiguration (SAA) [22]. The main difference between these methods lies in whether the IP address is generated by a server (DHCP/DHCPv6) or by the MH itself (IPv6 SAA). For cases where the MH is not concerned about the its IP address, but only requires the address to be unique and routable, IPv6 SAA is a preferred method for TraSH to obtain a new address since it significantly reduces the required signalling time.

B. STEP 2: Add IP addresses to association

When the SCTP association is initially setup, only the CN's IP address and the MH's first IP address (IP1) are exchanged between CN and MH. After the MH obtains another IP address (IP2 in STEP 1), MH should bind IP2 into the association (in addition to IP1) and notify CN about the availability of the new IP address.

SCTP provides a graceful method to modify an existing association when the MH wishes to notify the CN that a new IP address will will be added to the association and the old IP addresses will be probably be taken out of the association. The IETF Transport Area Working Group (TSVWG) is working on the "SCTP Address Dynamic Reconfiguration" Internet draft [23], which defines two new chunk types (ASCONF and ASCONF-ACK) and several parameter types (Add IP Address, Delete IP address, Set Primary Address, etc.). This option will be very useful in mobile environments for supporting service reconfiguration without interrupting on-going data transfers.

In TraSH, MH notifies CN that IP2 is available for data transmission by sending an ASCONF chunk to CN with parameter type set to 0xC001 (Add IP Address). On receipt of this chunk, CN will add IP2 to its local control block for the association and reply to MH with an ASCONF-ACK chunk indicating the success of the IP addition. At this time, IP1 and IP2 are both ready for receiving data transmitted from CN to MH.

C. STEP 3: Redirect data packets to new IP address

When MH moves further into the coverage area of wireless access network2, data path2 becomes increasingly more reliable than data path1. CN can then redirect data traffic to the new IP address (IP2) to increase the possibility of data being delivered successfully to the MH. This task can be accomplished by the MH sending an ASCONF chunk with the Set-Primary-Address parameter, which results in CN setting its primary destination address to MH as IP2.

The critical questions here are three-fold: (1) What kind of information should be used to trigger Set-Primary-Address, Layer 2, Layer 3 or Layer 4 handovers? (2) Who initiates Set-Primary-Address: CN or MH? (3) When is the right time to execute Set-Primary-Address? The answers to questions (2) and (3) depend largely on the answer to question (1). If MH can utilize the information from Layer 2, such as radio link Signal/Noise Ratio (SNR), Bit Error Rate (BER), or available bandwidth, MH has much more information than CN about whether the primary data path should be switched over to the new path. To compensate for the transmission/propagation delay from MH to CN, the MH can send the ASCONF chunk predictively at a time which is RTT/2 before the optimal switchover time. One disadvantage of this method is that it requires cross-layer communication in the protocol stack, which may result in difficulties in protocol deployment. If Layer 2 information is not available to MH, CN and MH should have the same knowledge about the link status. In this case, it may be preferable to let CN initiate the Set-Primary-Address by observing the packet loss pattern over the old data path; this will have the advantage of reducing the handover latency by RTT/2.

D. STEP 4: Updating the Location manager

TraSH supports location management by employing a location manager that maintains a database which records the correspondence between MH's identity and current primary IP address. MH can use any unique information as its identity, such as the home address (as in MIP), domain name, or a public key defined in the Public Key Infrastructure (PKI).

Following our example, once the Set-Primary-Address action is completed successfully, MH should update the location manager's relevant entry with the new IP address (IP2). The purpose of this procedure is to ensure that after MH moves from the wireless access network1 into network2, further association setup requests can be routed to MH's new IP address IP2. This update has no impact on existing active associations.

We can observe a important difference between TraSH and MIP: the location management and data traffic forwarding functions are coupled together in MIP, whereas they are *decoupled in* TraSH *to speedup handover and make the deployment more flexible*.

E. STEP 5: Delete or deactivate obsolete IP address

When MH moves out of the coverage of wireless access network1, no *new* or *retransmitted* data packets should be directed to address IP1. In TraSH, MH can notifies CN that

IP1 is out of service for data transmission by sending an ASCONF chunk to CN with parameter type set to 0xC002 (Delete IP Address). Once received, CN will delete IP1 from its local association control block and reply to MH with an ASCONF-ACK chunk indicating the success of the IP deletion.

A less aggressive way to prevent CN from sending data to IP1 is for the MH to advertise zero receiver window (corresponding to IP1) to CN [24]. This will give CN an impression that the interface (on which IP1 is bound) buffer is full and can not receive any more data. By deactivating, instead of deleting the IP address, TraSH can adapt more gracefully to MH's zigzag (often referred to as ping pong) movement patterns, and reuse the previously obtained IP address (IP1) as long as the lifetime of IP1 has not expired. This will reduce the latency and signalling traffic that would have otherwise been caused by obtaining a new IP address.

F. Timing diagram of TraSH

Fig. 2 summarizes the signalling sequences involved in TraSH. Here we assume IPv6 SAA and MH initiated Set-Primary-Address. Timing diagrams for other scenarios can be drawn similarly, but are not shown here because of space limitations.

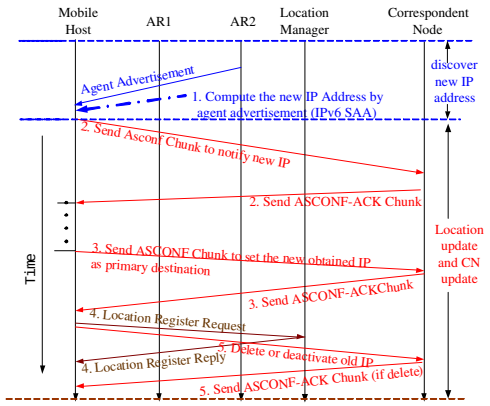


Fig. 2. Timeline of TraSH

In this figure, the numbers before the events correspond to the step numbers in Sec. III-A to III-E, respectively.

G. Vertical handover between different technologies

Different types of access network technologies can be integrated with each other to give mobile users a transparent view of the Internet. Handover is no longer only limited to between two subnets in WLAN, or between two cells in a cellular network (horizontal handover). In the future, mobile users will expect seamless handover between heterogeneous access networks (vertical handover).

Since MIP operates in Layer 3 and is independent of the underlying access network technology, MIP may be used in a heterogeneous environment. However, there are some disadvantages in using Mobile IP for vertical handovers [25].

TraSH is well suited to meeting the requirements of vertical handover. Fig. 3 illustrates an example of using TraSH to perform vertical handovers from WLAN to a cellular network, and then to a satellite network. The multi-homed mobile host in TraSH is equipped with multiple interface cards that can bind IP addresses allocated from different kinds of wireless network access technologies.

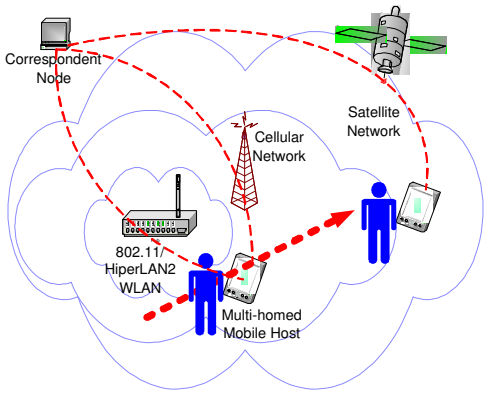


Fig. 3. Vertical handover using TraSH.

IV. Location Management and Data Transfer Path in TraSH

A. Location management

As mentioned in Sec. III-D, TraSH needs to setup a location manager for maintaining a database of the correspondence between MH's identity and its current primary IP address. Unlike MIP, the location manager in TraSH is not restricted to the same subnet as MH's home network (in fact, TraSH has not concept of home or foreign network). This will make the deployment of TraSH much more flexible than MIP.

When a location manager is used, the location management can be done in the following sequence as shown in Fig. 4:

1) MH updates the location manager with the current primary IP address.
2) When CN wants to setup a new association with MH, CN first sends a query to the location manager with MH's identity (home address, domain name, or public key, etc.)
3) Location manager replies to CN with the current primary IP address of MH.
4) CN sends an SCTP INIT chunk to MH's new primary IP address to setup the association.

If we use the domain name as MH's identity, then we can merge the location manager into a DNS server. The idea of using a DNS server to locate mobile users can be traced back to [26]. The advantage of this approach is its transparency to existing network applications that use domain name to IP address mapping.

Since MIP requires that the location management entity must reside on the HA, this location manager (DNS server) based method is not applicable to MIP. In contrast to MIP, TraSH *decouples location management from data traffic forwarding*, and hence can use this DNS server based location management. An Internet administrative domain can allocate one or more location servers for its registered mobile users.

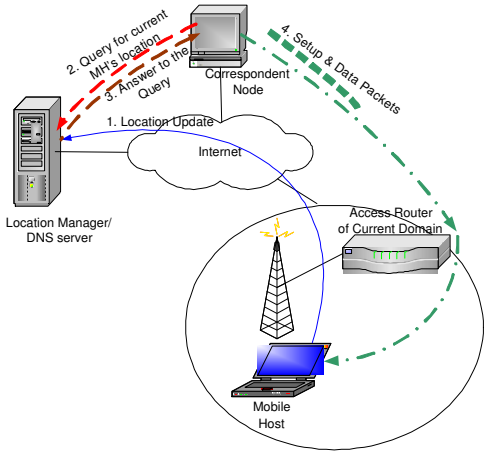


Fig. 4. Location management in TraSH

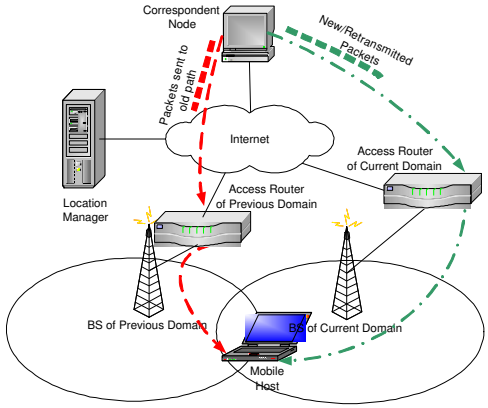


Fig. 5. Data transfer path after a TraSH handover.

Compared to MIP's requirement that each subnet must have a location management entity (HA), TraSH can reduce system complexity and operating cost significantly by not having such a requirement. TraSH, however, requires a mobile user to provide the IP address of the location manager when he/she publish his/her identity.

B. Data transfer path

The data transfer path after a TraSH handover is illustrated in Fig. 5. The difference between TraSH and MIP is that TraSH sends data packets directly to the MH instead of going through the HA. This eliminates the infamous triangular routing problem encountered in MIP. Note that, in TraSH, the retransmitted packets (due to packets lost during the handover) from CN should also be directed to MH's new IP address since the old IP address is very likely unreachable. In contrast to Mobile IP, there is no Home or Foreign agents; TraSH, however, requires a location manager for the CN to locate the current position of the MH when a new association setup is initiated by the CN.

V. Performance Comparison

In this section, we will present performance comparison results based on *ns-2* simulation. We have implemented the preliminary version of TraSH in *ns-2* simulator, and the *ns-2* patch for MIP [27] from U.C. Berkeley is used for simulating MIP's performance. To make a fair comparison, we have used SCTP as the transport protocol for both MIP and TraSH. Fig. 6 shows the network topology used for the simulation. The link bandwidth and propagation delay are listed along the links. An FTP source agent is attached to CN and a sink agent is attached at the MH. Each base station has a coverage of 40 meters in radius, and the overlapping region between two base stations is 10 meters. The MH moves between the two domains with a ping-pong style, with a handover frequency ranging from 5 to 30 handovers per minute.

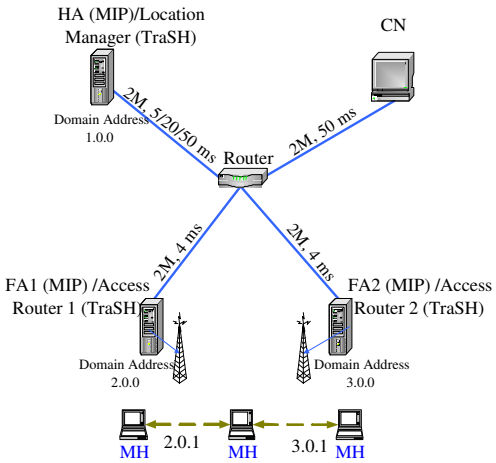


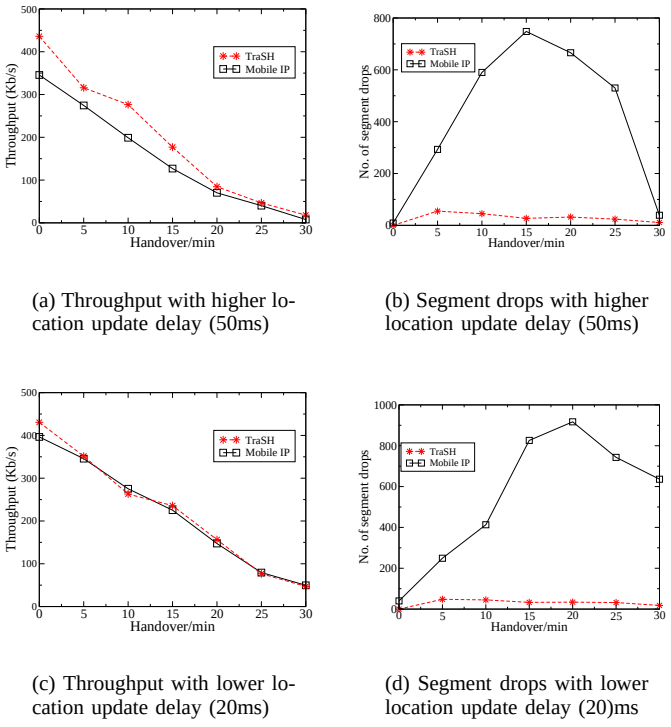
Fig. 6. Simulation topology.

Fig. 7(a) shows that when the location update delay (the delay between MH and HA in case of mobile IP, between MH and location manager in case of TraSH) is high, TraSH has an obvious higher throughput over MIP. This is because TraSH eliminated the tri-angular routing in MIP and in TraSH MH can receive packets arriving from the old path while registering through the new path. Also the segment drops caused by handover in TraSH is significantly less than in Mobile IP due to the TraSH's ability to receive packets coming from the old path during handover (see Fig. 7(b)).

When the location update delay is low, the throughput of MIP and TraSH is similar, due to the effect of triangular routing in MIP being less (see Fig. 7(c)). However, the segment drops in MIP is still noticeably higher than TraSH due to MIP's inability to receive packets in fly during the registration process (see Fig. 7(d)). In both Figs. 7(b) and 7(d), the segment drops first increase as the handover frequency increases; this is due to the preparation time for handover becoming less. The segment drops then decrease after a threshold; this is because of SCTP's congestion control taking the dominance and CN backing off to reduce packet losses.

VI. Security Considerations

The communication medium of mobile wireless environment is openly exposed to intruders, which makes the mobile network more vulnerable to malicious attacks than a wired network. A protocol supporting user mobility must consider associated security risks. In this section, we consider several security-related issues in TraSH.



(a) Throughput with higher location update delay (50ms)

(b) Segment drops with higher location update delay (50ms)

(c) Throughput with lower location update delay (20ms)

(d) Segment drops with lower location update delay (20)ms

Fig. 7. Performance Comparison of TraSH with MIP

A. Cooperation with Fire-walls and Ingress Filtering

As discussed in Sec. I, MIP requires firewall transversal solution [5] to resolve conflict with network security solutions. In TraSH, there is no such notion as home network, so the problem of fire-wall at the home network in MIP does not apply to TraSH.

TraSH has the advantage of not being affected by ingress filtering. This is because the MH uses the new IP address obtained from the new domain as its source IP address for outgoing packets. Since this source IP address belongs to the same subnet as the Border Router receiving the data packet, the Border Router does not activate Ingress Filtering, as is done in the case of MIP.

B. Dynamic address reconfiguration

TraSH needs to employ an SCTP option called Dynamic address reconfiguration (see Sec. III). The use of this option creates an extra security risk called *traffic-redirection attack*. An attacker "A" claims that its IP address should be added into an established association between "H_1" and "H_2", and that further communication should be directed to this IP address. Therefore, an IP authentication process needs to be employed for address reconfiguration signalling. IPSec and Internet Key Exchange (IKE) protocols were not initially designed to support multi-homed sessions efficiently; they need to create a separate database entry or perform a key negotiation for each pair of source/destination address, which is a waste of memory and time. IETF IPSec working group has a relevant standard (RFC 3554 [28]), which provides several functional requirements and recommendations for using IPSec and IKE with SCTP multi-homing.

VII. Conclusions

The Stream Control Transmission Protocol is a standard-track transport layer protocol proposed by IETF. This article introduces a new mobile handover scheme called TraSH, which utilizes the multi-homing feature of SCTP to keep the old data path alive while setting up the new data path. This scheme can cooperate with normal IPv4 or IPv6 infrastructure without the support of Mobile IP. Different aspects of the scheme are discussed including handover signalling procedure, location management, data transfer pathes, handover performance comparison with Mobile IP and security considerations.

References

[1] C. Perkins editor, "IP Mobility Support." IETF RFC 3344, August 2002.

[2] C. E. Perkins, "Mobile Networking Through Mobile IP," *IEEE Internet Computing*, vol. 2, no. 1, pp. 58–69, January/February 1998.

[3] Jarkko Sevanto, Mika Liljeberg, and Kimmo E. E. Raatikainen, "Introducing quality-of-service and traffic classes into wireless mobile networks," *Proceedings of the 1st ACM international workshop on Wireless mobile multimedia*, Dallas, Texas, pp. 21–29, 1998.

[4] "Low latency handoffs in Mobile IPv4." IETF DRAFT, draft-ietf-mobileip-lowlatency-handoffs-v4-07.txt, October 2003.

[5] G. Montenegro and V. Gupta, "Sun's SKIP firewall traversal for Mobile IP." IETF RFC 2356, June 1998.

[6] "Mobile IP regional registration." IETF DRAFT, draft-ietf-mobileip-reg-tunnel-04.txt, March 2001.

[7] "IP micro-mobility support using HAWAII." IETF DRAFT, draft-ietf-mobileip-hawaii-00.txt, June 1999.

[8] "Cellular IP." IETF DRAFT, draft-ietf-mobileip-cellularip-00.txt, December 1999.

[9] C.E. Perkins and K.Y. Wang, "Optimized smooth handoffs in mobile ip," *IEEE International Symposium on Computers and Communications*, pp. 340 –346, July 1999.

[10] M.C. Jung, J.S. Park, D.M. Kim, H.S. Park, and J.Y. Lee, "Optimized handoff management method considering micro mobility in wireless access network," *5th IEEE International Conference on High Speed Networks and Multimedia Communications*, pp. 182 –186, July 2002.

[11] I.W. Wu, W.S. Chen, H.E. Liao, and F.F. Young, "A seamless handoff approach of Mobile IP protocol for mobile wireless data networks," *IEEE Transactions on Consumer Electronics*, vol. 48, no. 2, pp. 335–344, May 2002.

[12] W. Liao, C.A. Ke, and J.R. Lai, "Reliable multicast with host mobility," *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1692 –1696, November 2000.

[13] "Mobility support in IPv6." IETF DRAFT, draft-ietf-mobileip-ipv6-24.txt, June 2003.

[14] "Hierarchical mobile ipv6 mobility management (HMIPv6)." draft-ietf-mipshop-hmipv6-00.txt, June 2003.

[15] R. Stewart and C. Metz, "SCTP: New transport protocol for TCP/IP," *IEEE Internet Computing*, vol. 5, no. 6, pp. 64–69, November/December 2001.

[16] A.L. Caro, J.R. Iyengar, and P.D. Amer et. al, "SCTP: a proposed standard for robust internet data transport," *IEEE Computer*, vol. 36, no. 11, pp. 56–63, November 2003.

[17] S. Fu and M. Atiquzzaman, "SCTP: State of the art in research, products, and technical challenges," *To appear in IEEE Communication Magazine*, March 2004.

[18] S. J. Koh, M. J. Lee, M. L. Ma, and M. Tuexen, *Mobile SCTP for Transport Layer Mobility*. draft-sjkoh-sctp-mobility-03.txt, February 2004.

[19] W. Xing, H. Karl, and A. Wolisz, "M-SCTP: Design and prototypical implementation of an end-to-end mobility concept," *5th Intl. Workshop The Internet Challenge: Technology and Applications*, Berlin, Germany, October 2002.

[20] L. Li, "PKI based end-to-end mobility using SCTP," *MobiCom 2002*, Atlanta, Georgia, USA, September 2002.

[21] A. Jungmaier, E.P. Rathgeb, and M. Tuxen, "On the use of SCTP in failover-scenarios," *International Conference on Information Systems, Analysis and Synthesis*, Orlando, Florida, pp. 363–368, July 2002.

[22] S. Thomson and T. Narten, "IPv6 stateless address autoconfiguration." IETF RFC 2462, December 1998.
[23] R. Stewart, M. Ramalho, and Q. Xie et. al., "Stream control transmission protocol (SCTP) dynamic address reconfiguration." draft-ietf-tsvwg-addip-sctp-06.txt, September 2002.
[24] T. Goff, J. Moronski, D. S. Phatak, and V. Gupta, "Freeze-TCP: A true end-to-end TCP enhancement mechanism for mobile environments," *IEEE INFOCOM*, Telaviv, Israel, pp. 1537–1545, March 2000.
[25] S. Dixit, "Wireless IP and its challenges for the heterogeneous environment," *Wireless Personal Communications*, pp. 261–273, August 2002.
[26] B. Awerbuch and D. Peleg, "Concurrent online tracking of mobile users," *ACM SIGCOMM Symposium on Communications, Architectures and Protocols*, pp. 221–233, September 1991.
[27] *Mobile IP Extensions to the ns Network Simulator*. www.icsi.berkeley.edu/ widmer/mnav/ns-extension/.
[28] S. Bellovin, J. Ioannidis, A. Keromytis, and R. Stewart, "On the use of stream control transmission protocol (SCTP) with IPsec." IETF RFC 3554, July 2003.