ISSN:0975-9646

SCTP over MIPv4 for Multi-homed Mobile Host

Surmila Thokchom[#], Thoudam Doren Singh[*]

[#]*Department of Information Technology, Xavier Institute of Engineering*
Mahim Causeway, Mumbai-16, India

[*]*Centre for Development of Advanced Computing (CDAC)*
Gulmohor Cross No 9, Juhu, Mumbai-400049, India

***Abstract*— The present paper reports on the experimentation using SCTP with mobile IP where mobile IP provides the device identification and location management support while SCTP takes care of the handoff management aspect. In this, we use multihoming feature of SCTP to allow mobile device to remain connected through multiple access networks simultaneously in an overlaid network environment. This make the handover smoother, reduces handoff latency and makes seamless mobility possible. The experimental results based on ns2 simulator is used to compare the performances of using multihomed SCTP for seamless handover and MIP4 for location management with MIP used for both handover and location management.**

Keywords*— Stream Control Transmission Protocol(SCTP), handover, transport layer, Mobile IP(MIP)

I. INTRODUCTION

In the recent times, the research on mobility support in IP networks has increased with the proliferation of laptops, hand-held computers, cellular phones and other mobile computing platforms connected to the Internet.
The most fundamental mobility [9] problem in IP-based networks is the separation of location and identity. This problem is solved at the network layer by Mobile IP. The Mobile IP supports host mobility at the network layer by deploying specially functioning routers (Home and/or Foreign Agents) into the network to keep track of current location of the mobile host and be able to route the packets destined for the mobile host to its current location by means of tunneling. This approach has two most serious shortcomings -limited performance and additional complexity for the network architecture.
Another approached is using the transport layer. The transport layer is considerably affected by mobility to be able to quickly adapt its flow and congestion control parameters to the new network situations during and after handovers. Thus, transport layer is the most promising candidate for mobility support. While TCP is indeed the most often used transport protocol in the Internet, it might not be the perfect platform to experiment with unconventional ways of supporting mobility. In particular, when considering the potential that a mobile terminal could be in contact with multiple access points at the same time, other protocols might offer a simpler starting point. A good candidate is the Stream Control Transmission Protocol (SCTP): an SCTP [6] "association" (essentially, a connection) can use multiple addresses simultaneously. While this property was not originally intended to support mobility (the rationale is to support highly available servers), it presents an excellent platform on which to experiment with new mobility-support mechanisms. In addition, many of its basic mechanisms such as flow and congestion control are very similar to TCP. Therefore, SCTP will be a solution to use as a starting point and introduce mobility support for it.

II. STREAM CONTROL TRANSMISSION PROTOCOL

The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) have been the only available transport layer protocols in the TCP/IP protocol suite. The TCP has been one of the reasons for the access of the Internet. Most application use TCP for end-to-end transport of data. For wired networks TCP has been very highly successful. However, with the advent of wireless networks and the profit rate of mobile computing paradigm, the inadequacies of TCP have begun to surface. Several deficiencies of TCP identified [6] were:

- TCP's strict by-order delivery gives rise to head-of-line (HOL) blocking in some applications.
- TCP is stream-oriented instead of being message-oriented.
- TCP can't support multi-homing, which is crucial in high availability environments such as SS7 signaling transport.
- TCP is vulnerable to blind denial of service (DoS) attacks by SYN segments.

To overcome the above limitations of TCP, a new transport protocol, called Stream Control Transmission Protocol (SCTP), was proposed by IETF in October 2000 to accomplish signaling transport. It was soon noticed that SCTP should be useful in a wider range of applications instead of just the signaling transport area.
The design of SCTP absorbed much strength that made TCP a success during the explosive growth of the Internet, such as the window based congestion control, error detection and retransmission, etc. Moreover, SCTP incorporated several new features that were not available in TCP. Two of the most prominent of these features, which have lot of relevance towards mobile computing, are Multihoming and Multistreaming.

A. Main Features of SCTP

The SCTP[6][8][11] resides in the transport layer of the Internet protocol stack as shown in Fig. 1[6] which also illustrates an SCTP association using Multihoming and Multistreaming.

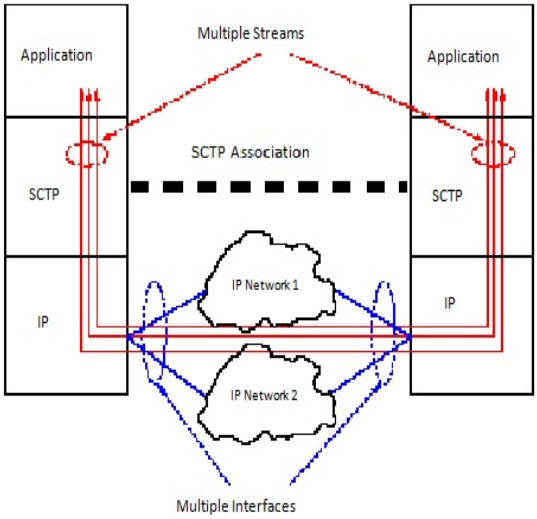

Fig 1: Schematic view of an SCTP association.

B. Multihoming

Multi-homing [6][8][11] allows an association between two end points to cross multiple IP addresses or network interface cards. For example, an SCTP multi-homing can have two endpoints say A and B which have two interfaces bound to the SCTP association. The two end points are connected through two kinds of links: satellite at the top and ATM at the bottom. One of the addresses is designated as the primary while the other one can be used as backup in the case of failure of the primary address, or when the upper layer application explicitly requests the use of the backup. Retransmission of lost packets can also be done over the secondary address. The built-in support for multi-homed endpoints by SCTP is especially useful in environments where applications require high-availability, such as SS7 signaling transport. The multi-homed SCTP associations can speed up the recovery from link failure situations without interrupting the data transfer.

C. Multistreaming

Multistreaming [6][8][11] is used to alleviate the head-of-line (HOL) blocking effect resulting from TCP's strict byte-order delivery policy. Each stream is a subflow within the overall data flow, and the delivery of each subflow is independent of each other.

Multi-streaming allows data from the upper layer application to be multiplexed onto one channel (called association in SCTP). Sequencing of data is done within a stream; if a segment belonging to a certain stream is lost, segments (from that stream) following the lost one will be stored in the receiver's stream buffer until the lost segment is retransmitted from the source. However, data from other streams can still be passed to the upper layer application. This avoids the head of line blocking (HOL) found in TCP where only one stream carries data from all the different upper layer applications.

This avoids the HOL blocking found in TCP, where a single stream carries data from all the upper-layer applications. In other words, the HOL effect is limited within the scope of individual streams, but does not affect the entire association.

III. MOBILE IP

A. Mobile IP Overview

Mobile IP[10] can be thought of as the cooperation of three major subsystems. First, there is a discovery mechanism defined so that mobile computers can determine their new attachment points (new IP addresses) as they move from place to place within the Internet. Second, once the mobile computer knows the IP address at its new attachment point, it registers with an agent representing it at its home network. Lastly, Mobile IP defines simple mechanisms to deliver datagrams to the mobile node when it is away from its home network.

Mobile IP introduces the following new functional entities.

Mobile Node: A host or router that changes its point of attachment from one network or subnetwork to another, without changing its IP address. A mobile node can continue to communicate with other Internet nodes at any location using its (constant) IP address.

Home Agent: A router on a mobile node's home network that delivers datagrams to departed mobile nodes, and maintains current location information for each.

Foreign Agent: A router on a mobile node's visited network that cooperates with the home agent to complete the delivery of datagrams to the mobile node while it is away from home. A mobile node has a home address, which is a long-term IP address on its home network. When away from its home network, a *care-of address* is associated with the mobile node and reflects the mobile node's current point of attachment. The mobile node uses its home address as the source address of all IP datagrams it sends, except where otherwise required for certain registration request datagrams (e&, see the fourth section). The following terms are frequently used in connection with Mobile IP.

Agent Advertisement: Foreign agents advertise their presence by using a special message, which is constructed by attaching a special extension to a router advertisement [8], as described in the next section.

Care-of Address: The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. There are two different types of care-of address: a foreign agent care-of address is an address of a foreign agent with which the mobile node is registered; a collocated care-of address is an externally obtained local address that the mobile node has associated with one of its own network interfaces.

Correspondent Node: A peer with which a mobile node is communicating. A correspondent node may he either mobile or stationary.

Foreign Network: Any networks other than the mobile node's home network.

Home Address: An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

Home Network: A network, possibly virtual, having a network prefix matching that of a mobile node's home

address. Note that standard IP routing mechanisms will deliver datagrams destined to a mobile node's home address to the mobile node's home network.

Mobility Agent: Either a home agent or a foreign agent.

Tunnel: The path followed by a datagram while it is encapsulated. The model is that, while encapsulated, a datagram is routed to a knowledgeable agent, which decapsulates the datagram and then forwards it along to its ultimate destination.

Virtual Network: A network with no physical instantiation beyond its router (with a physical network interface on another network). The router **(**e.g**,** a home agent) generally advertises reachability to the virtual network using conventional routing protocols.

Visited Network: A network other than a mobile node's home network to which the mobile node is currently connected.

Visitor List: The list of mobile nodes visiting **a** foreign agent.

B. Protocol Overview

Mobile IP is a way of performing three related functions:

- **Agent Discovery:** Mobility agents advertise their availability on each link for which they provide service.
- **Registration:** When the mobile node **is** away from home, it ***registers*** its care-of address with its home agent.
- **Tunneling:** In order for datagrams to be delivered to the mobile node when it is away from home, the home agent has to tunnel the datagrams to the care-of address.

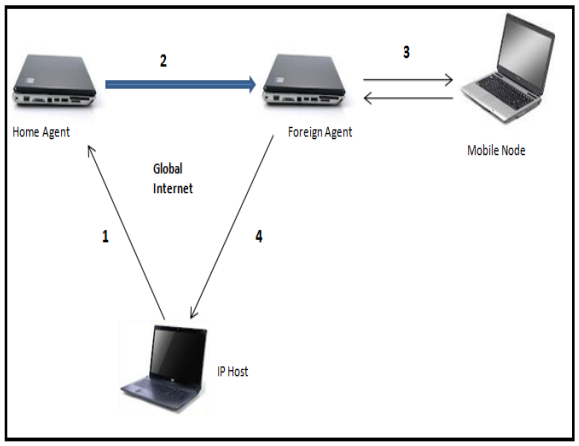

Fig: 2 Mobile IP datagram Flow.

The following outlined of operation of the Mobile IP protocol, as shown in Figure 2[10]

- Mobility agents make themselves known by sending agent advertisement messages. An impatient mobile node may optionally solicit an agent advertisement message.
- After receiving an agent advertisement, a mobile node determines whether it is on its home network or a foreign network. A mobile node basically works like any other node on its home network when it is at home.
- When a mobile node moves away from its home network, it obtains a care-of address on the foreign network, for instance, by soliciting or listening for agent advertisements, or contacting Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP).
- While away from home, the mobile node registers each new care-of address with its home agent, possibly by way of a foreign agent.
- Datagrams sent-to the mobile node's home address are intercepted by its home agent, tunneled by its home agent to the care-of address, received at the tunnel endpoint (at either a foreign agent or the mobile node itself), and finally delivered to the mobile node.
- In the reverse direction, datagrams sent by the mobile node are generally delivered to their destination using standard IP routing mechanisms, not necessarily passing through the home agent.

When the home agent tunnels a datagram to the care-of address, the inner IP header destination (i.e., the mobile node's home address) is effectively shielded from intervening routers between its home network and its current location. At the care-of address, the original datagram exits from the tunnel and is delivered to the mobile node.

It is the job of every home agent to attract and intercept datagrams that are destined to the home address of any of its registered mobile nodes. The home agent basically does this by using a minor variation on proxy Address Resolution Protocol (ARP), and to do so in the natural model it has to have a network interface on the link indicated by the mobile node's home address. If the home agent is the only router advertising reachability to the home network, but there is no physical link instantiating the home, network, then all datagrams transmitted to mobile nodes addressed on that home network will naturally reach the home agent without any special link operations.

The routing of datagrams to and from a mobile node away from home, once the mobile node has registered with its home agent is illustrated in Figure 2. The mobile node is presumed to be using a care-of address provided by the foreign agent:

- A datagram to the mobile node arrives on the home network via standard IP routing.
- The datagram is intercepted by the home agent and is tunneled, to the care-of address, as depicted by the arrow going through the tube.
- The datagram is detunneled and delivered to the mobile node.
- For datagrams sent by the mobile node, standard IP routing delivers each to its destination. In the figure, the foreign agent is the mobile node's default router.

IV. Experimental Results

A. Simulation Topology and Parameters

In this section, we describe the simulation topology and parameters that have been used to compare the performance of SCTP with multihomed features using MIP for location management and MIP with TCP. We have used ns-2.28 simulator that supports MIP and SCTP.

B. Simulation Topology

The network topology used in our simulations is shown in Fig 3. The setup consists of one Home agent (HA), four Foreign agents (FAs), one correspondent node (CN) and one Mobile node (MN) moving from its Home

Agent to overlapping region of FAs. In our experiment the domains of the mobility agents i.e. FAs overlap to assume the overlapping network area assumption. The link characteristics, namely the bandwidth (Megabits/s) and propagation delay (milliseconds), are shown on the links in the figure.

C. Simulation Parameters

We have used the following parameters in our simulations:

- A pair of FTP source is attached to the CN and MH, respectively, to transfer data from CN to MH.
- We have simulated AR (HA/FA) having a radio coverage area of 250meters in radius, and the overlapping region of 180metres and another radio coverage of 300 meters of 200meters.

In the experiments *Destination-Sequenced Distance-Vector* (DSDV) has been used as routing protocols.

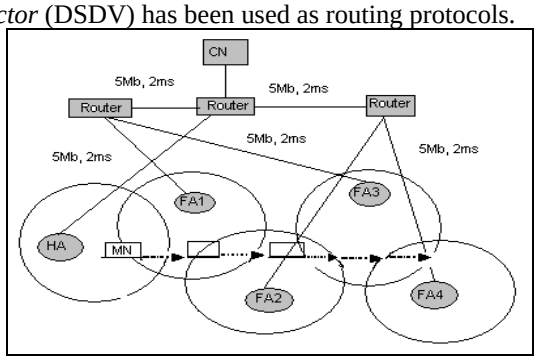

Fig :3 Experimental Setup

D. Performance Evaluation of the Scheme

We have evaluated the simulation through following criteria:

1. Graphs of Received packets vs time in different scenarios.
2. A table comparing the Handover Latency in different scenarios.

E. Simulation Results

i. Received Packets

We define the packet received as the number of received packets during the movement of the MN from HA and through FAs as shown in the above topology in experimental setup. We have compared the received packets during a period of time between MIP and SCTP and found on all scenarios that SCTP have significantly better performed than MIP. The results of the different scenarios are shown in terms of graph in figure 4, 5, 6, 7 respectively.

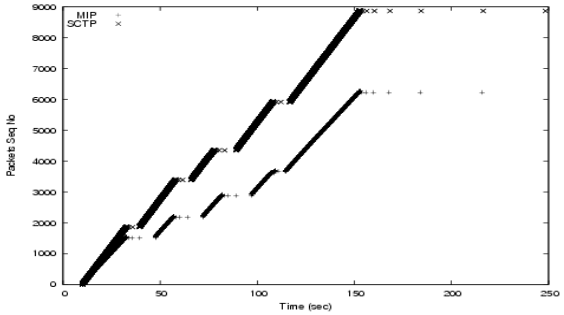

Fig 4: Packets Seq No. vs Time for MIP and SCTP having a range of 250metres radius and moving at 10m/s speed

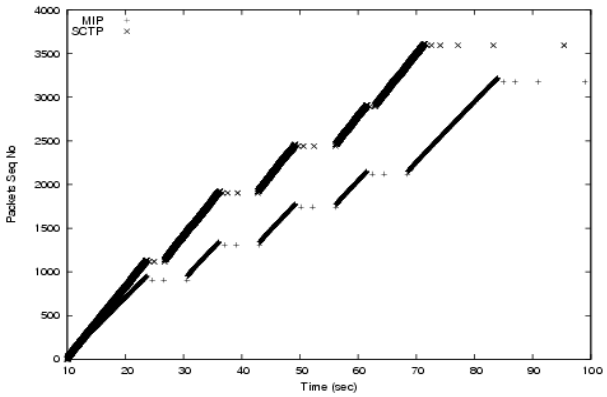

Fig 5: Packets Seq No. vs Time for MIP and SCTP having a range of 250metres radius and moving at 20m/s speed

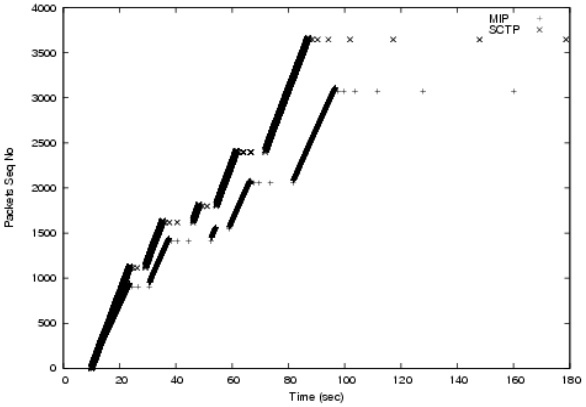

Fig 6: Packets Seq No. vs Time for MIP and SCTP having a range of 300metres radius and moving at 20m/s speed

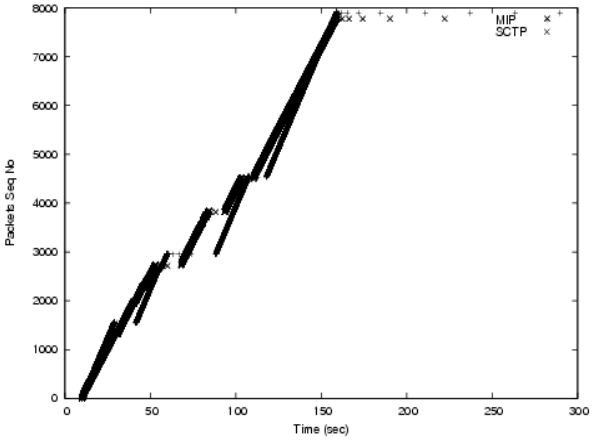

Fig 7: Packets Seq No. vs Time for MIP and SCTP having a range of 300metres radius and moving at 10m/s speed

ii. A Table showing comparative data of handover time.

We define the *handover latency* as the time interval between the last data segment received through the old path and the first data segment received through the new path from CN to MH. We also evaluated the performance with varying speed from 10 m/s to 20 m/s. The results are in Table 1.

TABLE 1
HANDOVER LATENCY

Range (radius in meters)	Speed (m/s)	Model	Average Handover Latency time (sec)
250	10	SCTP	3.79
		MIP	5.895
250	20	SCTP	8.2
		MIP	12.10
300	10	SCTP	6.3
		MIP	9.85
300	20	SCTP	7.85
		MIP	12.6

V. CONCLUSION

In this paper, we have presented a comparative study of MIP with TCP and SCTP with multi-homed features using MIP for location management. From experimental results, we conclude that SCTP gives significantly better performance than MIP in terms of packets received during a period of time and handover latency. In other words SCTP provides smoother handover, reduces the handover latency and makes seamless mobility.

We also highlight the future directions of the present experiment. In the present experiment, only one triggering method for comparing mobile node wireless strength with a threshold value was used. This can be upgraded by comparing wireless strength of the mobile node with respect to both the base station in case of dual homing and triggering the handover according to stronger signal strength.

We have experimented only for straight movement passing from one cell to another. Crossover movement can be experimented to see the performance degradation.

ACKNOWLEDGMENT

We would like to thank Prof. Dilip Kumar Saikia, CSE Department, Tezpur University for his valuable input.

REFERENCES

[1] M. Riegel and M. Tuxen, *Mobile SCTP*, February 2003, draft-riegeltuxexen-mobile sctp-02.txt.
[2] C. Perkins, Ed., *IP Mobility for IPv4* , August 2002, RFC 3344.
[3] Seok Joo Koh, *mSCTP with Mobile IP for Transport Layer Mobility*, August 2003, draft-sjkoh-mobile-sctp-mobileip-02.txt.
[4] Ilknur Aydin, Woojin Seok, Chien-Chung Shen, *Cellular SCTP: A Transport-Layer Approach to Internet Mobility*, 2003, IEEE.
[5] Seok Joo Koh, Moon Jeong Chang, and Meejeong Lee, *mSCTP for Soft Handover in Transport Layer, March 2004*, IEEE.
[6] Shaojian Fu and Mohammed Atiquzzaman, *SCTP: State of the art in Research, Products and Technical Challenges*,2003, IEEE.
[7] Tsuguo Kato, Ryuichi Takechi, Hideaki Ono, *A Study on Mobile IPv6 Based Mobility Management Architecture*, FUJITSU Sci. Tech. J.,37,1,(June 2001).
[8] Armando L. Caro Jr., Janardhan R. Iyengar et.al., *SCTP: A Proposed Standard for Robust Internet Data Transport*, 2003, IEEE computer society.
[9] Wesley M. Eddy, *At What Layer Does Mobility Belong?* , 2004, IEEE.
[10] Charles E. Perkins, *MOBILE IP*, IEEE Communications Magazine, May 2002.
[11] Randall Stewart and Chris Metz, *SCTP: New Transport Protocol for TCP/IP*, IEEE, 2001.