Performance of SCTP in Wi-Fi and WiMAX networks with multi-homed mobiles

Vicuña Nelson
INRIA and LIA/Université d'Avignon
339, chemin des Meinajaries,
84911 Avignon, France
nelson.vicuna@etd.univ-avignon.fr

Jiménez Tania
LIA/Université d'Avignon
339, chemin des Meinajaries,
84911 Avignon, France
tania.jimenez@univ-avignon.fr

Hayel Yezekael
LIA/Université d'Avignon
339, chemin des Meinajaries,
84911 Avignon, France
yezekael.hayel@univ-avignon.fr

ABSTRACT

This paper provides an exhaustive performance analysis by simulation of the SCTP transfer protocol in WiMAX and Wi-Fi networks. We provide also a comparison of SCTP with both transfer protocols UDP for "VoIP-like" applications and TCP for FTP sessions, as SCTP can support these two types (elastic and non-elastic) of traffic. Finally, we study how SCTP performs when a mobile is multi-homed, i.e. connected simultaneously to two wireless networks (Wi-Fi and WiMAX).

Categories and Subject Descriptors

C.2.5 [**Computer-Communication Networks**]: Local and Wide-Area Networks; C.2.6 [**Computer-Communications Networks**]: Standards; C.4 [**Performance of Systems**]: Performance attributes

General Terms

SCTP, performance, wireless, NS-2

Keywords

Wireless, SCTP, NS-2, VoIP, Multi-homing.

1. INTRODUCTION

The Stream Control Transmission Protocol (SCTP) has similar congestion control and retransmission mechanisms to those of TCP, which were designed for wired networks.

Wireless networks have some particularities that can create problems when adaptive protocols as TCP and SCTP are used, such as high latency and higher packet loss than wired networks. SCTP and TCP have been developed to work in wired networks, where the latency and the packet loss are low. In this case, if a packet is lost, both protocols assume that dropped is due to congestion instead of a possible collisions in the radio access medium. SCTP and TCP see that as a congestion problem and reduce the sending rate.

We study the performance of SCTP in wireless networks to see the behavior of this protocol with different parameters and compare it with other transport protocols, like TCP and UDP. We used two types of traffic: elastic (the rate of flows adjusts to the available bandwidth, i.e, FTP transfers or HTTP) and non-elastic (traffic that cannot support large delay variabilities as VoIP).

We use NS-2 to study SCTP through extensive simulations. We compare the behavior of the three transport protocols (SCTP, UDP, and TCP) over three different technologies (Wired, IEEE 802.11 and IEEE 802.16) as well as multi-homing between the two wireless technologies.

Flexibility and diversity of modules in NS-2 allows us to design heterogeneous scenarios evaluating their performance. We made the necessary adjustments in the source code to achieve the interconnection of the modules and operation between them. Modules like SCTP of Protocol Engineering Laboratory (PEL) at the University of Delaware, WiMAX and Wi-Fi extentions developed at the National Institute of Standards and Technology (NIST) of the United States, have been used at the same time with different kinds of traffic and topologies to do the performance evaluation study.

The rest of this paper is organized as follows. In section 2, we have a short description of SCTP with an emphasis on the differences it has with respect to TCP and UDP. In section 3, the simulation scenarios are explained and in section 4 the performance analysis is presented. In section 5, we provide an overview of the related work in SCTP performance evaluation and compare it with our work. Finally, section 6 concludes the paper.

2. SCTP

SCTP is a transport protocol defined in RFC4960 [15]. It was designed by the Signaling Transport (SIGTRAN) group of the Internet Engineering Task Force (IETF). Initially, it was introduced to serve as a reliable signaling and control transport protocol for telecommunications traffic running over IP networks via a number of proposed adaptation layers, but has since evolved for more general use to satisfy the needs of applications that require a message-oriented protocol with all the necessary TCP-like mechanisms [4].

Table 1 compares a summary of SCTP's services and features with those of TCP and UDP. SCTP provides sequenc-

WNS2, October 24, 2008, Athens, Greece
Copyright ©2008 ICST ISBN # 978-963-9799-31-8.

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358

Table 1: Comparison of SCTP, TCP, and UDP[17]

Protocol Feature	SCTP	TCP	UDP
State required at each endpoint	yes	yes	no[1]
Reliable data transfer	yes	yes	no
Congestion control and avoidance	yes	yes	no
Message boundary conservation	yes	no[2]	yes
Path MTU discovery and message fragmentation	yes	yes[2]	no
Message bundling	yes	yes[2]	no
Multi-homed hosts support	yes	no	no
Multi-stream support	yes	no	no
Unordered data delivery	yes	no	yes
Security cookie against SYN flood attack	yes	no	no
Built-in heartbeat (reachability check)	yes	no[3]	no

ing, flow control, reliability and full-duplex data transfer like TCP. In addition, SCTP has unique features including *multi-homing* and *multi-streaming*. Based on these two features, SCTP was originally designed to provide a reliable transport between two end hosts using multiple, independent control of streams. SCTP offers new delivery options, ideal for non-elastic traffic as shown in [17], SCTP is also richer in functionality and more tolerant to network and component failures than TCP.

An SCTP association provides novel services such as multi-homing and multi-streaming as we can see in sections 2.3 and 2.4. At the bottom of the Figure 1, we can see an architecture that includes two network interfaces per host. Two paths are provided through the independent networks, these two paths would be collected into an association. At the top is a TCP connection. Each host includes a single network interface; a connection is created between a single interface on each node. Upon establishment, the connection is bound to each interface.

2.1 SCTP Congestion Control

The congestion control algorithms used by SCTP are based on TCP Congestion Control described in RFC2581 [1] and is always applied to the entire association, and not to individual streams.

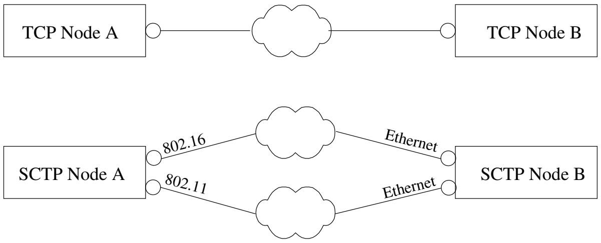


Figure 1: An SCTP Association vs. a TCP Connection

The congestion control mechanism of SCTP consists of slow-start, congestion avoidance and fast retransmit algorithms. The endpoints maintain three variables to regulate data transmission rate: receiver advertised (*rwnd*), congestion window (*cwnd*) and slow-start threshold (*ssthresh*). SCTP also requires an additional control variable, which is used during congestion avoidance to facilitate *cwnd* adjustment, *partial_bytes_acked* (*pba*) [15, 18].

SCTP sets a Transmission Sequence Number (TSN) to each data fragment or unfragmented message. The TSN is independent of any Stream Sequence Number established at the stream level. The receiving through the Selective Acknowledgement (SACK), acknowledges all TSNs received, despite the existence of gaps in the sequence. In this way, reliable delivery is kept separate from sequenced delivery. Each SACK acknowledges the Cumulative TSN and can also contain one or more Gap ACK blocks. By definition, all TSNs acknowledged by Gap ACK Blocks are greater than the value of the Cumulative TSN ACK as described in section 3.3.4 of [15, 18].

Slow-start. As we can see in [15], the slow-start algorithm is used to probe the network to determine the available capacity at the beginning of a transfer, or after repairing loss detected by the retransmission timer. During the slow-start phase, when a SACK chunk is received, the value of *cwnd* is increased by the total size of the acknowledged DATA chunks. The result is that *cwnd* increases exponentially, doubling every RTT. The complete rules can be check in section 7.2.1 of [15, 18].

Congestion Avoidance. When the value of *cwnd* is greather than *ssthresh*, SCTP changes its behavior to the congestion avoidance algorithm. In this phase, the *cwnd* is increased by at most 1*MTU per RTT. The complete rules are written in section 7.2.2 of [15, 18]. During congestion avoidance of SCTP, *cwnd* can only be increased when the full *cwnd* is utilized [5].

Fast Retransmit on Gap Reports. Fast retransmit is used when a single DATA chunk with TSN=i is dropped. It consists to retransmit the DATA chunk i when the SACKs show that several other DATA chunks sent after DATA chunk i have already arrived, while the DATA chunk i is still unacknowledged. In this way we can avoid the time-out of the retransmission timer. In SCTP, due to its compulsory use of Gap ACK Blocks, if a TSN is not acknowledged in 4 consecutive received SACKs in [18] or 3 consecutive received SACKs in [15] while any other newer TSN is acknowledged in any Gap ACK Block of those 3 or 4 SACKs, the TSN must

[1] With UDP a node can communicate with another node without going through a setup procedure or changing any state information. This is called connection-less, but in reality each UDP packet has the needed state within it to form a connection so that no ongoing state needs to be maintained at each endpoint.

[2] Because TCP treats all the data passed from its upper layer as a formatless stream of data bytes, it does not preserve any message boundaries. However, due to its byte-stream-based nature, TCP can automatically resize all the data into new TCP segments suitable for the Path MTU before transmitting them.

[3] Most TCP implementations do implement a “keep-alive” mechanism. This mechanism is very similar to the SCTP heartbeat, with the main difference being the time interval used. In TCP the “keep-alive” interval is, by default, set to two hours. The goal of this “keep-alive” is long-term state cleanup, which is in sharp contrast to SCTP’s much more rapid heartbeat, which is used to aid in fast failover.

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358

be retransmitted. Moreover, both *cwnd* and *ssthresh* variables are set to one half of the value of *cwnd* in the moment of the fast retransmission. For a more detailed explanation, the reader may refer to section 7.2.4 of [15, 18].

Fast Recovery. The fourth algorithm used for congestion control is fast recovery, defined in [1] and used in TCP right after a fast retransmission. TCP without the SACK option can not inform the data sender about anything else but the last data segment received in order. This implies many duplicated ACK. In order to solve this problem TCP can anticipate it, increasing the *cwnd* when the duplicate acknowledgements are still arriving. As noted in [1], this artificially increase the *cwnd* in order to reflect the additional segment that has left the network. This is basically the fast recovery algorithm. SCTP, however, does not need that algorithm due to its use of Gap ACK Blocks.

2.2 Differences between SCTP and TCP

Gap ACK Blocks in the SCTP SACK carry the same meaning as the TCP SACK in [11]. TCP and SCTP consider the information carried in the SACK by TCP and in the Gap ACK Blocks in the SACK chunk by SCTP as advisory information. In SCTP, any DATA chunk that has been acknowledged by SACK is not considered completely delivered until the Cumulative TSN ACK Point passes the TSN of the DATA chunk. The value of *cwnd* controls the amount of outstanding data. SCTP SACK leads to different implementations of Fast Retransmit and Fast Recovery than those in non-SACK TCP [15, 18].

The major differences[1] between SCTP and TCP congestion control algorithms are:

1. *cwnd*, is suggested to be at least $2 * MTU$ in SCTP, which is usually $1 * MTU$ in TCP.

2. SCTP is required to be in slow-start phase when the slow-start threshold, *ssthresh*, is equal to the *cwnd*. In TCP, it is optional to be either in the slow-start phase or in the congestion avoidance phase when the *ssthresh* is equal to the *cwnd*. In NS-2 when the slow-start threshold is equal to the *cwnd* the congestion avoidance phase is used.

3. In SCTP, the increase of the *cwnd* is controlled by the number of acknowledged bytes; in TCP, it is controlled in general by the number of new acknowledgement received.

4. In SCTP, fast retransmission is triggered by the 4th missing report of a chunk; in TCP, three duplicate ACKs trigger fast retransmission.

5. SCTP has no explicit fast recovery algorithm, in contrast to TCP.

2.3 SCTP Multi-homing

As indicated by the authors in [6], unlike SCTP, TCP requires only one source and one destination IP address for each connection. SCTP associations support host with multiple IP addresses, i.e. multi-homing. When initiating an association, the lists of all IP addresses with its port numbers is done by each endpoint. In this way, the SCTP sender and receiver are able to identify the IPs that has a same number of port.

Normally, the SCTP sender transmits through a selected primary destination address and the rest of the addresses are considered as alternate paths. This alternate paths are used during a link failure situation through the built-in support for multi-homing that allows switch over to other destination address without stopping the data transfer.

Multiple active interfaces may imply the existence of different paths between the multi-homed hosts. However, RFC 4960 does not allow a sender to simultaneously send new data on multiple end-to-end paths; SCTP maintains a primary destination to which all new transmissions are sent; nevertheless, retransmissions are sent to alternate destinations, as is indicated in [7].

In this paper, in the case of multi-homing, we use these multiple paths between multi-homed source and destination hosts through Concurrent Multipath Transfer (CMT) proposed by [7] to increase throughput for a network application. CMT transfers data, concurrently, from a source host to a destination host using the multi-homing feature of SCTP. The CMT algorithm choose the destination path in a round-robin way, beginning with the primary destination address. The destination path is changed when *cwnd*, for a given path, does not allow sending more data.

2.4 SCTP Multi-streaming

Multi-streaming separates and transmits application data in streams. These streams have the capacity of independent and sequenced delivery. This has an advantage, if message loss occurs in one stream, other streams are unaffected. On the other hand, in TCP, a stream is a sequence of bytes that ensures the delivery in “strict sequence”. The disadvantage of this sequence delivery is that the bypass among streams is not permissible [6].

3. SIMULATIONS

We used four different scenarios to evaluate the performance of SCTP. All of them have clients in one side, and servers in the other side, and share a bottleneck link (dumbbell topology). The main difference is the technology used for the connection of the clients to the bottleneck. The bandwidths used in the bottleneck were less than 2Mbps to evaluate and compare the performance of SCTP and TCP in the presence of congestion.

1. A Wired scenario is proposed as reference. Both TCP and SCTP were designed for wired networks. We want to know the behavior of both protocols in its natural scenario.

2. IEEE 802.11 (Wi-Fi)

3. IEEE 802.16 (WiMAX)

4. Multi-homing Wi-Fi and WiMAX

The parameters used for the simulation in NS-2.29 are the following:

- Three types of traffic:

[1] This differences between TCP and SCTP are based on the RFC2960 [18] due to the implementation of SCTP in NS-2, contributed by the University of Delaware, is based on this RFC. It should be noted that at present, most of the implementations of SCTP use the RFC2960 (i.e, GNU/Linux Kernel 2.6.24

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358

- Elastic Traffic, which are File Transfer Protocol (FTP) flows. We used the values of FTP parameters used in [13]. The size of downloaded files is generated according to a Pareto distribution with average of 80KB (small files or mouses) and 800KB (big files or elephants) and 1.18 of shape; The inter-request time per client is exponential with average of 90 seconds.
- Non-elastic Traffic, is represented by Voice over IP (VoIP) like data traffic: Bi-directional ON-OFF traffic generated on the basis of G.729. The holding time is exponentially distributed with an average of 30 seconds for short calls and 300 seconds for long calls. The interval between two calls is exponentially distributed with average of 60 seconds.
- Noise (exogenous) ON-OFF traffic: Exponentially distributed ”on” and ”off” durations with rate of 40Kbps per client during the ”on” period. The ”on” and ”off” average durations are 100ms. In the direction clients to servers.

- TCP version: Newreno
- Simulation Time: 3600 seconds
- Client Data Rate: 100 Mbps (Wired Network), 54 Mbps (Wi-Fi), 22 Mbps (WiMAX)
- Server Data Rate: 100 Mbps
- WiMAX modulation: OFDM 64QAM 3/4
- Routing protocol for wireless topologies: No Ad-Hoc Routing Agent (NOAH).
- The path MTU: 1500 bytes
- SCTP associations data chunk: 1468 bytes.

Three similar topologies have been used for simulating the proposed scenarios. An initial topology for the wired network (see Fig. 2), another for wireless networks Wi-Fi and WiMAX (see Fig. 3), and another one for multi-homing wireless networks Wi-Fi and WiMAX (see Fig. 4).

The advantage of an open-source simulator as NS-2 is that it allows us to integrate different modules and to modify them if there are problems on the interconnection of some modules. We make changes in the source code of the SCTP module for using exponential traffic over SCTP, in order to simulate the non-elastic traffic.

3.1 Simulated Topologies

3.1.1 Wired Topology

We used the topology shown in Figure 2 to simulate a wired network. This topology supports n_1 FTP clients for TCP connections or SCTP associations, n_2 “VoIP-like” clients (UDP connections or SCTP associations) simultaneously and n_3 noise clients.

$N0_{i=1..3,j=0..n_i}$ are destination nodes, and $N1_{i=1..3,j=0..n_i}$ are the source nodes or servers. The link between nodes $n0$ and $n1$ is the bottleneck with a bandwidth of 2Mbps and 10ms of propagation delay. The clients and the servers, at each side of the bottleneck act as a local area network. All the connections or associations have random RTT uniformly distributed between $42ms$ and $624ms$.

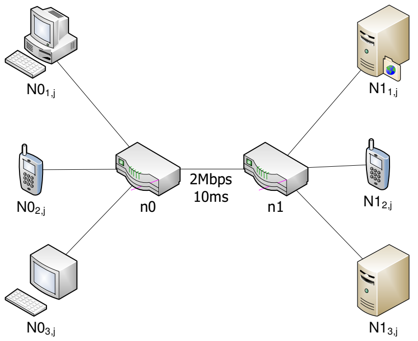


Figure 2: Wired Topology

3.1.2 Wireless Topology (802.11 and 802.16)

We used the topology shown in Figure 3 to simulate the wireless network. Like the previous topology, it supports n_1 TCP connections or SCTP associations simultaneously for FTP, n_2 UDP connections or SCTP associations simultaneously for “VoIP-like” data and n_3 noise clients.

$N0_{i=1..3,j=0..n_i}$ are destination nodes, and $N1_{i=1..3,j=0..n_i}$ are the source nodes or servers. BS node, is the base station to which client nodes are associated. The link between node BS and $n1$ is the bottleneck; the bandwidth of the link is 2Mbps and has 10ms of propagation delay. The wireless clients are uniformly distributed in the space. For the implementation in NS-2, we used a hierarchical structure based on 2 domains and one cluster for each domain.

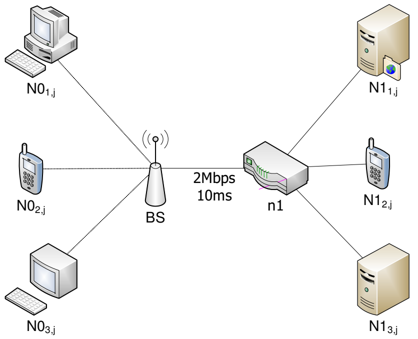


Figure 3: Wireless 802.11 and 802.16 Topology

Depending on the type of wireless networks, BS and the client nodes are configured to provide the physical environment adapted to Wi-Fi or WiMAX[2].

3.1.3 Wireless Multi-homing Topology (802.11 and 802.16)

We used the topology shown in Figure 4 to simulate the wireless multi-homing network. This topology supports n_1 SCTP associations simultaneously for FTP clients, n_2 SCTP associations simultaneously for “VoIP-like” data and n_3 noise clients.

$N0_{i=1..3,j=0..n_i}$ are destination nodes, and $N1_{i=1..3,j=0..n_i}$

[2] For Wi-Fi and WiMAX implementation in NS-2, we used the module developed by the National Institute of Standards and Technology (NIST)[12].

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358

are the source nodes or servers. Each $N0_{i,j}$ node has 2 interfaces, $N0WiFi_i$ and $N0WiMAX_i$; one in order to establish the connection with Wi-Fi and the other one for WiMAX. The $BSWiFi$ and $BSWiMAX$ nodes are the base stations to which client nodes are associated. The link between node $n0$ and $n1$ is the bottleneck link with a bandwidth of 2Mbps and 10ms of propagation delay. Wireless clients are uniformly distributed in the space. A hierarchical structure was used in the NS-2 implementation with three domains. One cluster for the servers nodes, one cluster for the multi-homing client nodes and three clusters for the access points and multi-homing interfaces of the clients nodes.

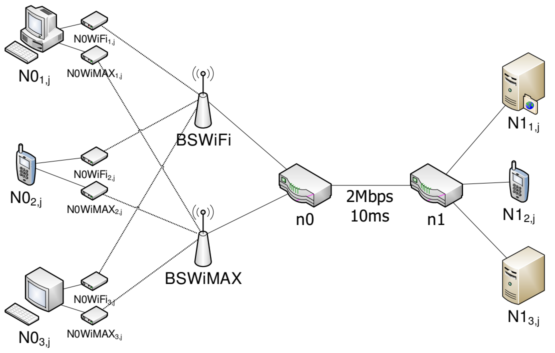


Figure 4: Wireless IEEE 802.11 and IEEE 802.16 Multi-homing topology

3.2 Performance Measures

We consider here three performance measures: Throughput, Delay, and Packet loss.

3.2.1 Throughput

We measure the average amount of data per second per client that is delivered over the bottleneck from the node $n1$ to the node $n0$.

3.2.2 Delay

We measure the average time that a packet of data takes in the queue of the bottleneck from the node $n1$ to the node $n0$.

3.2.3 Packet loss

Packet loss is due to network congestion. Packets are dropped in the bottleneck when the packet queue is full. We measure the rate of packets dropped in the bottleneck from the node $n1$ to the node $n0$.

3.3 Simulation scenarios

We simulate each transport protocol in each technology (Wired, Wi-Fi and WiMAX). We used TCP or SCTP for FTP and UDP or SCTP for "VoIP-like" data. We used the Partial Reliability Extention described in the RFC3758 [16] when we send data using SCTP for "VoIP-like" data. This extension of SCTP avoids the retransmission of VoIP data through the implementation of a new SCTP packet (Forward Cumulative TSN, FORWARD TSN), "used by the data sender to inform the data receiver to adjust its cumulative received TSN point forward because some missing TSNs are associated with data chunks that should not be transmitted or retransmitted by the sender" as noted in section 3.2 of [16].

We have hence the following combinations of protocols and applications:

- **TCP/UDP**: TCP for FTP and UDP for "VoIP-like" data,
- **TCP/SCTP**: TCP for FTP and SCTP for "VoIP-like" data,
- **SCTP/UDP**: SCTP for FTP and UDP for "VoIP-like" data,
- **SCTP/SCTP**: SCTP for FTP and SCTP for "VoIP-like" data.

In multi-homing Wireless Wi-Fi and WiMAX topology we used only SCTP as transport protocol for both applications, FTP and "VoIP-like" data (SCTP/SCTP).

We simulate each combination 10 times with different random seeds. The results showed are the average of these ten replications. In Table 2 we show the values of the parameters used for the different simulation scenarios, for each combination of transport protocol in each topology.

In the scenario A the number of FTP clients varies from 0 to 50 by steps of 5 clients. The number of clients of VoIP varies from 0 to 50 in the scenario B also by steps of 5. We introduced noise traffic in scenario C and varied its number from 0 to 100 by steps of 10. These clients sent traffic in the ACK direction. In the scenario D we vary the ratio small/big file size, by steps of 10%. In the scenario E we vary the proportion of short duration calls and long duration calls by steps of 10% as well. In scenario F the buffer queue size varies from 5 to 50 packets by steps of 5. In the last scenario (G), we took as bandwidth of the bottleneck the values 250kbps, 500kbps, 1000kbps and 2000kbps.

4. PERFORMANCE EVALUATION

We compare in all scenarios (A to G), the three performance measures: throughput, delay and packet loss.

4.1 Throughput for elastic traffic

We observe on figure 5(a) and 5(d) that as TCP is more aggressive than SCTP, the mean throughput of one FTP session is better with TCP in all topologies when the number of FTP clients is small (less than 20). Conversely, the SCTP protocol gives a better throughput when the number of FTP clients is high (more than 20). We explain this phenomenon by, in a low loaded network, aggressiveness of TCP allows to obtain more bandwidth but, in a heavy loaded network, this aggressiveness implies less bandwidth because there is too much packet drops (see figure 7(a)).

When the number of VoIP clients is important (see figure 5(e)), the UDP protocol for VoIP application overloads the Wi-Fi access channel and produces a fall of the TCP or SCTP throughput for FTP application. By using SCTP protocol for VoIP application, this phenomenon does not appear and the throughput of FTP application is stable as the number of VoIP clients increases. Moreover the packet drops and the mean delay for a VoIP client are not so much degraded using SCTP instead of UDP in every topology (see figure 6(a) for Wi-Fi topology and figure 6(d) for WiMAX topology).

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358

Table 2: Values of parameters in each simulation scenario

Simulation Scenario	FTP Clients	VoIP Clients	Noise Clients	FTP average File Size (KB)	VoIP average call duration (sec.)	Bottleneck Queue Size	Bottleneck Bandwidth (Kbps)
A	0-50	10	0	50% 80 50% 800	50% 30 50% 300	25	2000
B	10	0-50	0	50% 80 50% 800	50% 30 50% 300	25	2000
C	10	10	0-100	50% 80 50% 800	50% 30 50% 300	25	2000
D	10	10	0	0%-100% 800 100%-0% 80	50% 30 50% 300	25	2000
E	10	10	0	50% 80 50% 800	0%-100% 300 100%-0% 30	25	2000
F	10	10	0	50% 80 50% 800	50% 30 50% 300	5-50	2000
G	10	10	0	50% 80 50% 800	50% 30 50% 300	25	250-2000

Then we can conclude with this study on the throughput for elastic traffic, that SCTP is less aggressive when the network supports more and more traffic than the protocol UDP when it is used for VoIP application.

4.2 Delay for non-elastic traffic

In both wireless topologies Wi-Fi (see figure 6(b)) and WiMAX (see figure 6(e)), the average per packet delay of VoIP application increases with the file size of FTP transfers. But we observe that this mean delay is lower when the non-elastic traffic uses SCTP instead of UDP. This difference is up to 30% less when all FTP transfer has 800 KB in the WiMAX topology and still 25% in the Wi-Fi one.

Considering the scenario E when the proportion of long call increases, the mean packet delay of VoIP application is apparently surprising because it decreases, in both wireless topologies Wi-Fi (see figure 6(c)) and WiMAX (see figure 6(f)). Indeed, the number of FTP clients is fixed to 10 and as the proportion of long VoIP session increases, more non-elastic packets are present in the queue proportionally to elastic traffic packet generated by FTP applications. Moreover, the number of VoIP simultaneous sessions increases. Then, the mean packet delay of VoIP application consequently decreases.

4.3 Drop for elastic traffic

Comparing the packet drops for elastic traffic with SCTP or TCP, we observe on figure 7(c) for Wi-Fi topology, that the packet drop is in fact increasing with the queue size when using TCP and decreasing when using SCTP. This comes from the aggressiveness of the slow-start congestion avoidance mechanism. Indeed, in TCP, the congestion window is doubled in terms of packets at each acknowledgement whereas in SCTP it is doubled in terms of bytes as seen in section 2.1. Moreover, the used of delayed ACK by SCTP will reduce the number of ACKs, which in turn slows the *cwnd* growth rate. This implies that more TCP packets are dropped during burst of losses, because a burst of data (i.e, a file transfer) can potentially cause a large amount of segment loss during the slow-start congestion avoidance phase than using SCTP.

This implies also that the throughput of FTP application is better using TCP than SCTP (see figure 5(c) in a Wired topology or figure 5(f) in a Wi-Fi topology). Thus there exists a compromise between loss and throughput between TCP and SCTP for elastic traffic.

4.4 Drop for non-elastic traffic

Comparing the packet drops for non-elastic traffic with SCTP or TCP, we observe in wireless Wi-Fi topology (see figure 8(b)) that the packet drop is less when we used UDP as transport protocol for VoIP and SCTP as transport protocol for FTP application. When the number of VoIP client is high (more than 20) we observe a decrease of the packet drops when we used TCP as transport protocol in FTP applications. This behavior is due to the Wi-Fi's contention-based access.

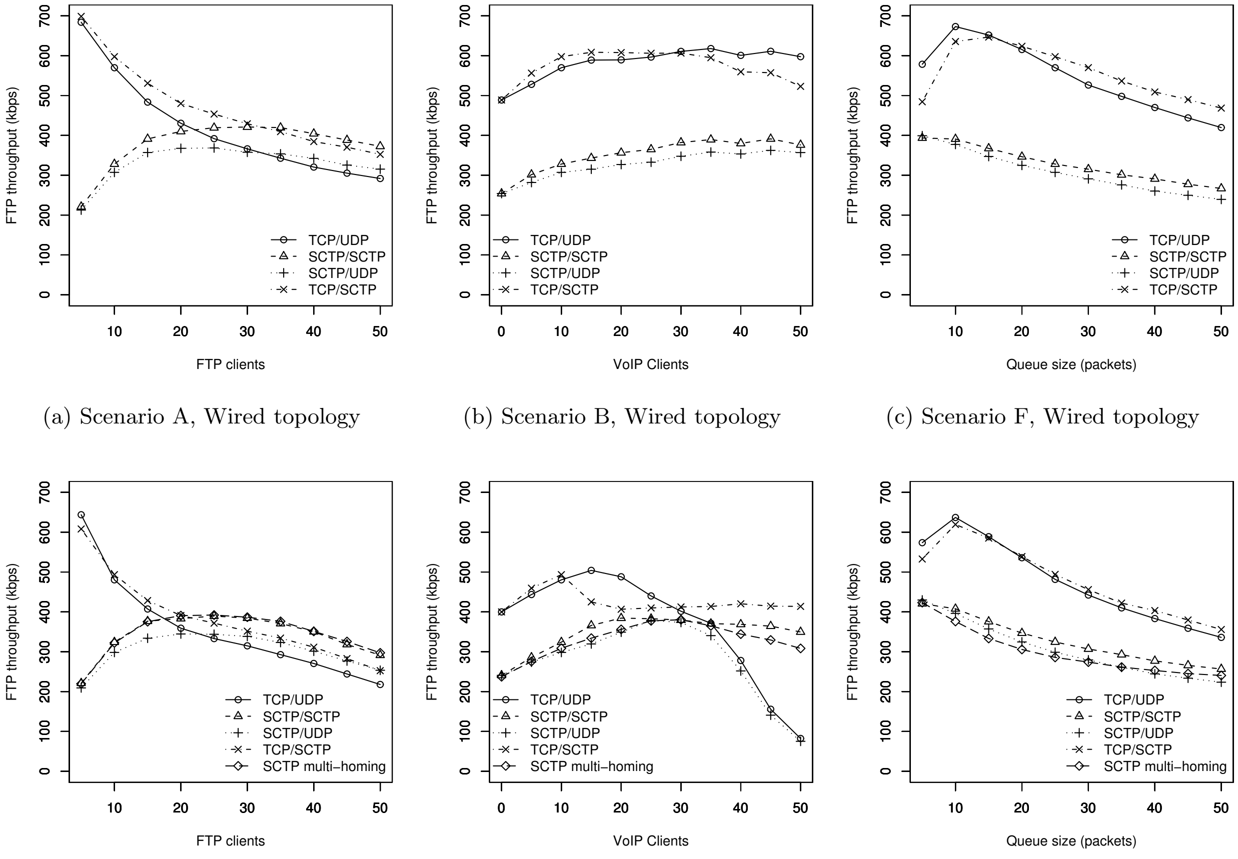
In the case of Wired (see figure 8(a)) and WiMAX (see figure 8(c)), UDP has a better behavior than SCTP as transport protocol of non-elastic traffic. Increasing VoIP clients, the increase in the percentage of losses is lower than when we used SCTP. In contrast to Wi-Fi, the MAC layer of Wired and WiMAX provide grant/request access, avoiding collisions, managing the resources of the wired or wireless link in an efficient way.

4.5 Multi-homing

We observe on figures 6(e) and 6(f) that the non-elastic traffic delay is lower when each mobile is connected simultaneously to WiMAX and Wi-Fi (multi-homed) compared to a connection with a single wireless technology. Concurrent connections between two different wireless technologies allows mobiles to access also Wi-Fi which has better performance than WiMAX. Then a multi-homed mobile connected simultaneously to Wi-Fi and WiMAX has better performance (delay, drop and throughput) than connected to only WiMAX (see figure 9(c)). We observe also that multihoming does not perform well compared with only Wi-Fi (see figure 5(f), 7(c) and 9(b) for examples). This behavior is due to packet dropping in Wi-Fi (see figure 7(a)), which is less than packet dropping in WiMAX (see figure 7(b)) taking the Wi-Fi interface as primary destination. That is why the CMT algorithm selects more frequently the Wi-Fi interface.

On the other hand, when the Wi-Fi access channel is overload (i.e, when the clients who sent traffic in the ACK di-

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358



(a) Scenario A, Wired topology

(b) Scenario B, Wired topology

(c) Scenario F, Wired topology

(d) Scenario A, Wi-Fi topology

(e) Scenario B, Wi-Fi topology

(f) Scenario F, Wi-Fi topology

Figure 5: Elastic traffic throughput

rection, are upper than 50, see figure 9(a)) the throughput in the multi-homing topology remains stable, because it remains sending data by the WiMAX interface.

5. RELATED WORK

In the last few years, many studies have been done in evaluating the performance of several aspects of SCTP. For example, a study of the coexistence of SCTP and TCP in the Internet has shown that SCTP traffic is TCP friendly in the sense that it has the same impact on the congestion control of other TCP connections as normal TCP traffic [8]. This study is different than ours in two ways: i. it is an experimental study, constrained to a small number of clients and only wired technology; ii. The authors only use elastic traffic. We too observe in our simulations a TCP-friendly behavior of SCTP.

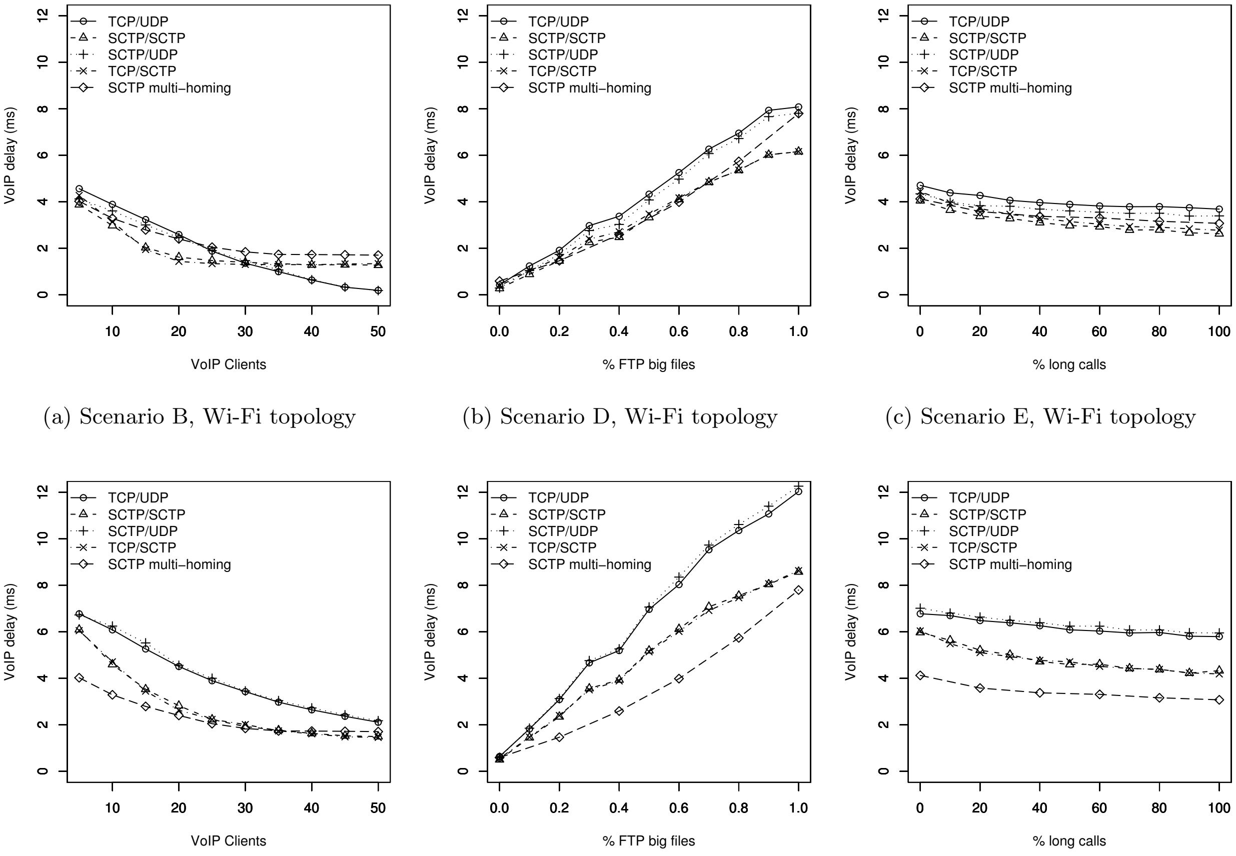
In [3] the authors focus on SCTP multi-streaming for reducing the latency of streaming multimedia in high-loss environments. They show that multi-streaming results in slower degradation in the network throughput as the loss rate increases than in TCP. Additionally, user satisfaction is increased with the improved multimedia quality provided by this feature. Similar results were obtained in our simulations when the loss rate increases (i.e, when we increase the number of FTP clients) despite using a single stream.

Using NS-2, in [9], the authors study the multi-streaming and the multi-homing SCTP features. They prove that these features have advantages over TCP in their scenario. They define the optimal number of streams in multi-streaming and explain how it affects network performance. In our work, multi-homing's advantage is observed when we have a high-number of packets losses in a network (i.e, Wi-Fi) because the alternative pathway (i.e, WiMAX) minimize the impact of packets drops.

In [14] the authors compare the performance of SCTP and TCP with respect to Web traffic concluding that SCTP can help to reduce the latency and improve the throughput. This is also true in our scenario when the number of clients is larger than 20.

In [10] the authors provide a simulation-based performance comparison of SCTP vs TCP in MANET environments. They found that SCTP and TCP have similar behavior in MANETs environment, but TCP outperforms SCTP in most cases due to the aditional overhead present in SCTP. Certainly the size of the header is an important factor, especially when we use applications such as VoIP. SCTP header

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358



(a) Scenario B, Wi-Fi topology

(b) Scenario D, Wi-Fi topology

(c) Scenario E, Wi-Fi topology

(d) Scenario B, WiMAX topology

(e) Scenario D, WiMAX topology

(f) Scenario E, WiMAX topology

Figure 6: Non-elastic traffic delay

size is bigger than the header used by UDP. As a result, we have a greater use of resources by SCTP and therefore a non-optimal use of them.

In [2] the authors presented their simulation results regarding the performance of SCTP in a wireless ad-hoc network environment under two routing protocols: DSR and AODV. They proposed a set of modifications to the SCTP protocol for handling pro-actively route failures in mobile ad-hoc networks and they showed that the transport layer allows for faster path selection, in the case that a number of paths exist, leading thus to improve overall throughput. We used NOAH as routing protocol, but we did not investigate the route failures.

In [19], the authors have shown that SCTP multi-homing can provide better throughput performance and more robustness in the wireless multi-access scenario, based on the Linux kernel experimentation. Similar results were obtained in our simulations studies.

In [5] the authors introduce the main features of SCTP and discuss the state of the art in SCTP research and development activities. They also provide a useful survey of the available products that use SCTP.

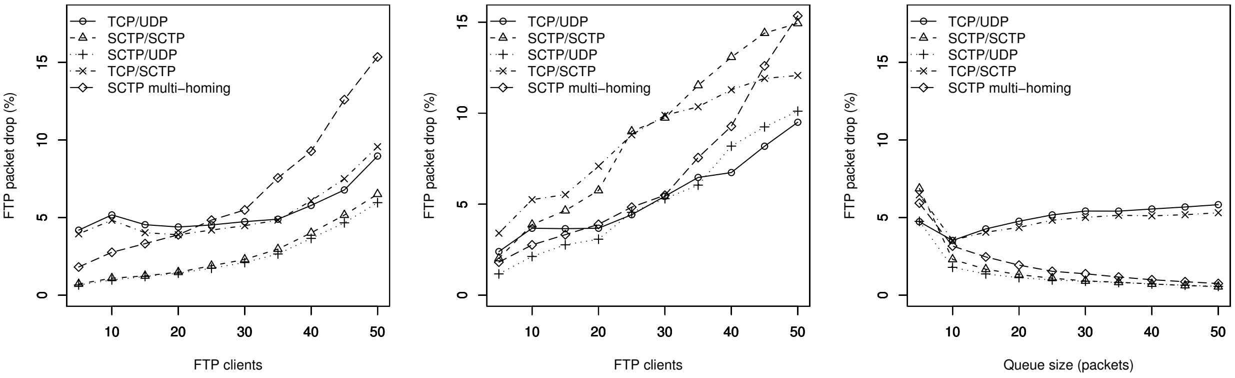
As far as we know, there is no reference on the use of SCTP over WiMAX. In this article we give some initial ideas on the behavior of SCTP over WiMAX. Further work is being done with more emphasis on WiMAX.

6. CONCLUSIONS

In this paper we presented a comparative study of SCTP with TCP over three different technologies: wired, Wi-Fi and WiMAX as well as multi-homing between the two wireless technologies. We simulate seven different scenarios in each technology, varying the parameters by small steps. In total we executed more than 80 different simulations. Each of them was executed ten times with different random seeds.

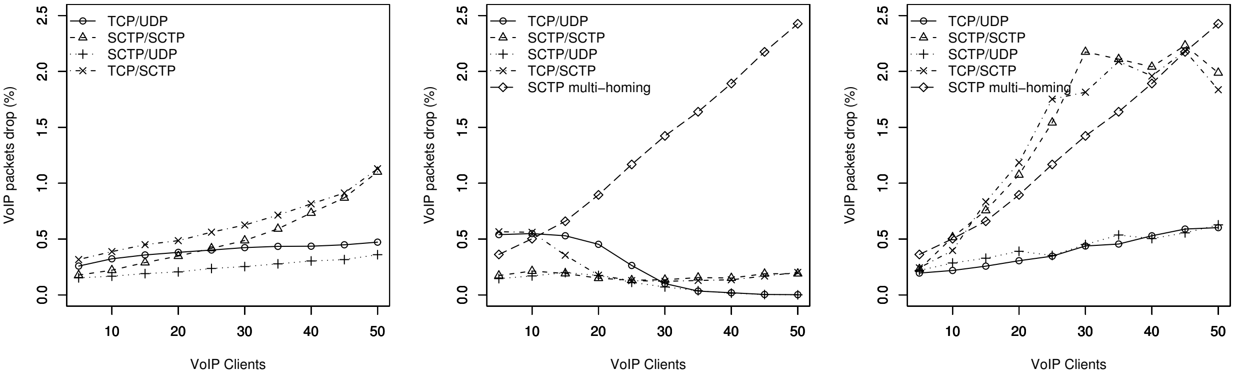
The different simulations proposed in this paper show a similar behavior between SCTP and TCP. However, TCP is more aggressive handling the congestion window. SCTP congestion control was designed similar to that of TCP with the goal to assure that SCTP does not behave more aggressively than TCP. When there are few competing flows TCP has better throughput, because it opens the window much quicker than SCTP, and so it take the available bandwidth quicker. On the other hand, when the number of flows is high, SCTP has better throughput than TCP. SCTP has smaller delay and packet loss than TCP which results in

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358



(a) Scenario A, Wi-Fi topology (b) Scenario A, WiMAX (c) Scenario F, Wi-Fi topology

Figure 7: Elastic traffic packet drop



(a) Scenario B, Wired Topology (b) Scenario B, Wi-Fi Topology (c) Scenario B, WiMAX

Figure 8: Non-elastic traffic packet drop

better performance in throughput, despite the lack of aggressiveness in handling the window congestion.

In non-elastic traffic, as VoIP, SCTP's behavior is as expected. However, the header of SCTP, is much larger than that of UDP, and hence consumes much more resources.

Contrary to what was expected with multi-homing, the use of CMT did not improve the throughput of the primary link. However, when we observe a collapse of the primary interface, there is no degradation in the throughput due to the use of a second link. Multi-homing in this case, behaves as a backup mechanism as originally proposed in RFC2960.

This study enables us to identify interesting problems to explore in future work. We plan to evaluate the performance of SCTP with wireless losses including other performance measures as jitter. We plan to study in depth the use of SCTP in WiMAX.

7. ACKNOWLEDGMENTS

The work of the first author was supported by the EuroFGI and EuroNF network of excellence. The work of the two other authors was partly supported by the French ANR project WiNEM: ANR-06-TCOM-05.

8. REFERENCES

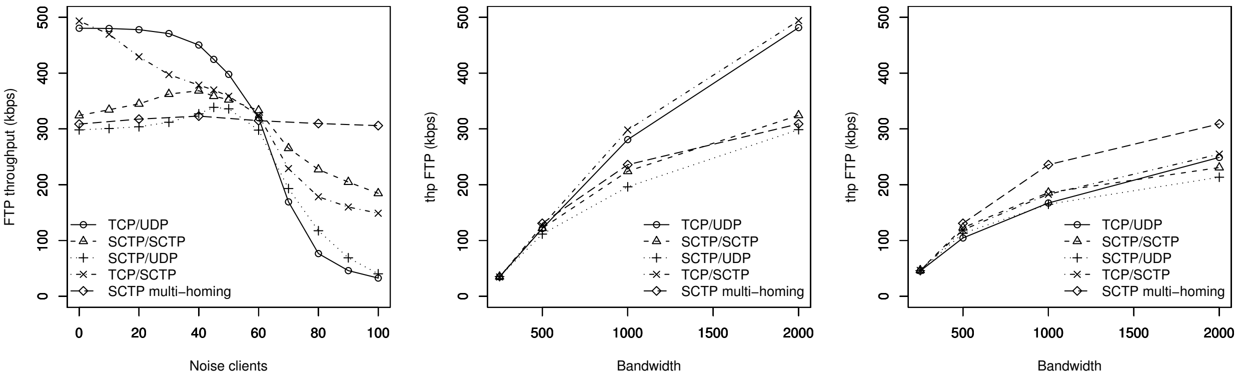
[1] M. Allman, V. Paxson, and W. Stevens. TCP Congestion Control. RFC 2581 (Proposed Standard), Apr. 1999. Updated by RFC 3390.

[2] A. Argyriou and V. Madisetti. Performance evaluation and optimization of sctp in wireless ad-hoc networks. In *Proceedings of 28th Annual IEEE International Conference on Local Computer Networks*, pages 317–318, October 2003.

[3] A. Caro Jr and P. Amer. Improving Multimedia Performance over Lossy Networks via SCTP, 2000.

[4] L. Coene. Stream Control Transmission Protocol Applicability Statement. RFC 3257 (Informational), Apr. 2002.

[5] S. Fu and M. Atiquzzaman. SCTP: State of the Art in Research, Products, and Technical Challenge. *IEEE Communications Magazine*, 42(4):64–76, April 2004.



(a) Scenario C, Wi-Fi Topology

(b) Scenario G, Wi-Fi Topology

(c) Scenario G, WiMAX

Figure 9: Elastic traffic throughput

[6] M. N. Islam and A. Kara. Thriughput analysis of sctp over multi-homed association. In *CIT '06: Proceedings of the Sixth IEEE International Conference on Computer and Information Technology*, page 110, Washington, DC, USA, 2006. IEEE Computer Society.

[7] J. Iyengar, K. Shah, P. Amer, and R. Stewart. Concurrent multipath transfer using sctp multihoming. In *Proceedings of International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, July 2004.

[8] A. Jungmaier, M. Schopp, and M. Tüxen. Performance Evaluation of the Stream Control Transmission Protocol. In *Proceedings of the IEEE Conference on High Performance Switching and Routing*, pages 141–148, Heidelberg, Germany, June 2000.

[9] S. Kang and M. Fields. Experimental study of the sctp compared to tcp. Technical report, Department of Electrical Engineering of Texas AM University, 2003.

[10] A. Kumar, L. Jacob, and A. L. Ananda. Sctp vs tcp: Performance comparison in manets. In *Proceedings of 29th Annual IEEE International Conference on Local Computer Networks*, pages 431–432, November 2004.

[11] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow. TCP Selective Acknowledgment Options. RFC 2018 (Proposed Standard), Oct. 1996.

[12] National Institute of Standards and Technology. Seamless and secure mobility. http://www.antd.nist.gov/seamkessandsecure.shtml.

[13] E. Noel and K. W. Tang. Performance analysis of a voip access architecture. In *ICPPW '04: Proceedings of the 2004 International Conference on Parallel Processing Workshops*, pages 282–290, Washington, DC, USA, 2004. IEEE Computer Society.

[14] S. K. R. Rajamani and N. Gupta. Sctp versus tcp: Comparing the performance of transport protocols for web traffic. Technical report, Computer Sciences Department of University of Wisconsin Madison, July 2002.

[15] R. Stewart. Stream Control Transmission Protocol. RFC 4960 (Proposed Standard), Sept. 2007.

[16] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen, and P. Conrad. Stream Control Transmission Protocol (SCTP) Partial Reliability Extension. RFC 3309 (Standard Track), May 2004.

[17] R. Stewart and Q. Xie. *Stream Control Transmission Protocol (SCTP): A Reference Guide*. Addison-Wesley Professional, 2002.

[18] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. Stream Control Transmission Protocol. RFC 2960 (Proposed Standard), Oct. 2000. Obsoleted by RFC 4960, updated by RFC 3309.

[19] J. Yuehui and H. H. Dajiang. Experimental Performance Studies of SCTP in Wireless Access Networks. In *Proceedings of ICCT2003*, pages 392–395, Beijing, China, April 2003.

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4358
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4358