A Performance Improvement Scheme of Stream Control Transmission Protocol over Wireless Networks

Kiwon Hong[1], Kugsang Jeong[1], Deokjai Choi[1], and Choongseon Hong[2]

[1] Computer Science Department, Chonnam National University
300 Yongbong-dong, Buk-gu, Gwangju, 500-757, Korea
{kiwon77,handeum}@iat.chonnam.ac.kr, dchoi@chonnam.ac.kr
[2] Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Yongil, Gyeonggl, 449-710, Korea
cshong@khu.ac.kr

Abstract. Today's computer network is shifting from wired networks to wireless networks. Several attempts have been made to assess the performance of TCP over wireless networks. Also, several solutions have been proposed to improve its performance. Many people believe SCTP would be replacement of TCP. However, the performance enhancement research for SCTP over wireless network is in beginning stage yet. In this paper we have measured performance characteristics of SCTP, and compared with ones of TCP and TCP-snoop over wireless network. After this experiment, we found the performance of SCTP is better than TCP, but worse than TCP-snoop. To improve the performance of SCTP over wireless network, we modified SCTP code by adopting TCP-snoop approach. We named it SCTP-snoop. With this SCTP-snoop, we experimented again, and found that it showed the best performance over wireless network among TCP, TCP-snoop, and SCTP.

1 Introduction

For the past 20 years, most Internet applications are implemented using TCP or UDP. But, those protocols are not good enough for multimedia traffics that are getting popular these days. In such background, SCTP was proposed by Internet Engineering Task Force and it was published as RFC 2960 in October 2000 as a Proposed Standard [1].

Like TCP, SCTP offers a point-to-point, connection-oriented, reliable delivery transport service for applications communicating over an IP network. It inherits many of the functions developed for TCP over the past two decades, including powerful congestion control and packet loss recovery functions. Also multiple stream mechanism of SCTP is designed to solve the head-of-the-line blocking problem of TCP, and association mechanism (the exchange of at least four SCTP packets) of SCTP is designed to solve the classic SYN flooding-type of denial-of-service attack of TCP [2].

Today Internet users are increasing rapidly. Also, various service extensions of mobile communication providers and increasing of mobile communication users require not only voice transmission, but also data transmission for various services. A communication service market will be changed from wired networks to wireless net-

O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3480, pp. 195 – 203, 2005.

works and to the consolidation trend of wired and wireless networks. So, data communication demands are increasing rapidly.

An original TCP was optimized in wired networks. It is not customized to the wireless networks, and it has many defects for wireless networks such as frequent cutoff and high error rate. So, if TCP is used over wireless networks, efficient transmission will not be guaranteed. Since wireless networks are less stable than wired networks, it experiences frequent packet loss. It affects RTT time, and TCP understands the network is in congestion state. According to the TCP retransmission policy, it will reduce the traffic and get slow down retransmission time too. It will affect the general performance of network [3].

To overcome that problem of TCP, researchers have proposed modified protocols actively such as Indirect-TCP and TCP-Snoop. But, in case of SCTP that is believed to be a next generation transport protocol, there has not been substantial effort to improve performance over wireless networks.

The Snoop protocol is a simple and efficient protocol for end-to-end communication [4]. Therefore we modified Snoop protocol for SCTP over wireless networks. The Snoop Agent is implemented on a base station (BS) that connects wired networks and wireless networks. We evaluate performance of SCTP-snoop in terms of required time to transmit certain amount of data, and the experiment shows that the performance of SCTP-snoop is better than TCP or SCTP over wireless networks.

This paper is organized as follows: In section 2, we present differences between SCTP and TCP congestion control. Section 3 describes a snoop protocol. In section 4, our simulation results and analysis are presented. Section 5 discusses future work and provides some conclusions.

2 Differences Between SCTP and TCP Congestion Control

The congestion control of SCTP is based on TCP's principles and it uses the SACK extension of TCP. It also includes slow start, congestion avoidance, and fast retransmission. There are subtle differences between the congestion control mechanisms of TCP and SCTP. The congestion control properties of SCTP that are different from those of TCP are as follows [5]:

1. The congestion window (cwnd) is increased according to the number of bytes acknowledged, not the number of acknowledgements received. Similarly, the flightsize variable, that represents how much data has been sent but not acknowledged on a particular destination address, is decreased by the number of bytes acknowledged. While in TCP, it is controlled by the number of new acknowledgement received.

2. The initial congestion window is suggested to be 2*MTU in SCTP, which is usually one MTU in TCP.

3. SCTP performs congestion avoidance when cwnd >ssthresh(slow start threshold). It is required to be in slow start phase when the ssthresh is equal to the cwnd. It is optional in TCP to be either in the ssthresh or in the congestion avoidance phase when the ssthresh is equal to the cwnd.

4. SCTP's Fast Retransmit algorithm is slightly different from TCP's. SCTP has no explicit fast recovery algorithm that is used in TCP. In SCTP, the parameter

Max.Burst is used after the fast retransmit to avoid flooding the network. Max.Burst limits the number of SCTP packets that may be sent after processing the SACK, which acknowledges the data chunk that has been fast retransmitted.

5. An unlimited number of GAP ACK blocks are allowed in SCTP. TCP allows a maximum of three SACK blocks

3 Snoop Protocol

The snoop is a TCP aware link layer protocol. Snoop was designed so that the wired infrastructure of the network would need no changes. Since Snoop protocol does not require changing wired network, it is good candidate for our system [4].

So, we modified snoop protocol for SCTP which means it supports multi-homing and multi-stream.

To support the multi-homing and the multi-streaming of SCTP, SCTP-Snoop agent executes followings: SCTP interchanges INIT Chunk and INIT-ACK Chunk, which are needed information for multi-homing and multi-streaming, during association establishment. In the process of exchange, SCTP-Snoop agent gets and stores addresses of Sender and receiver included INIT Chunk and INIT-ACK Chunk. If the packet losses have occurred by receiver, SCTP-Snoop agent will judge a problem by a transmission path. So, SCTP Snoop transfers lost packets by selecting one of transmission paths. Also, SCTP Snoop checks lost chunks through Gap Ack Block field of SCTP SACK-Chunk, and retransmits lost chunks stored in buffer.

The snoop module has two linked procedures, snoop_data() and snoop_ack(). Snoop_data() processes and caches packets intended for the mobile host(MH) while snoop_ack() processes acknowledgments (ACKs) coming from the MH and drives local retransmissions from the base station to the mobile host. The flowcharts summarizing the algorithms for snoop_data() and snoop_ack() are shown in Figure 1 and Figure 2 , and their working details are described in brief below.

In figure 1, when the data chunk packet is received by base station with snoop agent, if it is not the new data chunk which is adjudged through the Transmission Sequence Number (TSN) of SCTP, the agent forwards it to the receiver without storing to buffer.

If it is the new data chunk and an out-of-sequence, the agent forwards it to the receiver after marking packet loss by congestion. If it is the new SCTP packet and in order, it copies into buffer and forwards it to the receiver. At that time, if the new SCTP packet is INIT-Chunk or INIT-ACK chunk, Snoop agent could store addresses into buffers after verification address parameters. And Snoop agent stores INIT-Chunk and INIT-ACK chunk into buffers and forwards to MH.

In figure 2, when the SCTP sack chunk is received by base station, if it is the new sack chunk, the agent removes it from the buffer and modifies retransmission timer by measuring RTT to reflect new RTT, while if it is the first duplicate sack chunk, it means packet loss in wireless networks. So, Snoop agent retransmits lost chunks after verification Gap Ack block of SCTP SACK-Chunk and dumps the duplicate sack chunk. However, if it is not the first duplicate sack chunk but the duplicate sack chunk, the agent dumps the duplicate sack chunk.

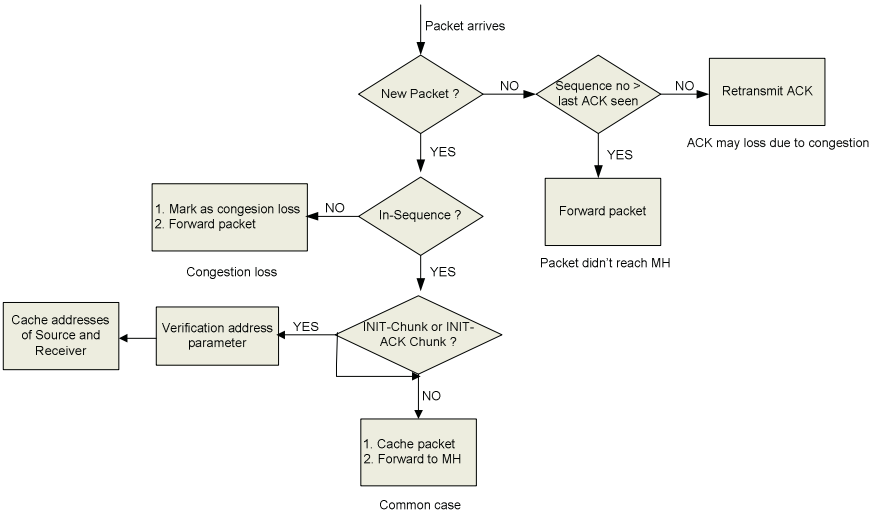

Fig. 1. Snoop_data()

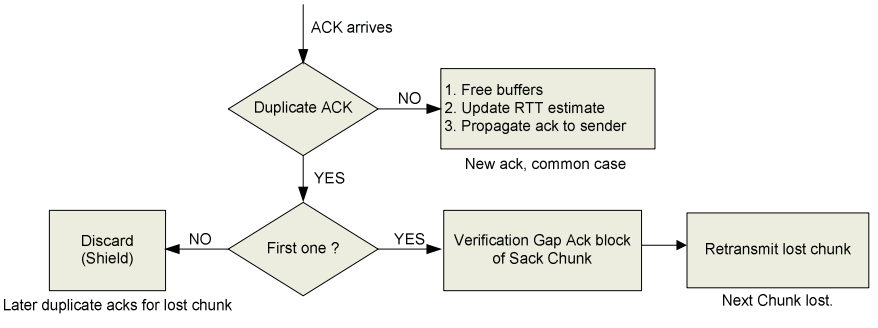

Fig. 2. Snoop_ack()

4 Performance Evaluation and Analysis

We estimated SCTP performance through comparison with original TCP which currently have been used as an transfer protocol for reliable transmission.

4.1 Simulation

All of the simulation results presented in this paper were obtained from an implementation of SCTP for the ns-2 simulation environment, which was developed by UC

Berkeley [6]. The SCTP module for ns-2 was developed by the Protocol Engineering Lab at the University of Delaware and is available as third party module [7].

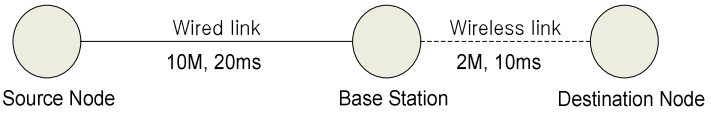

Fig. 3. Network Topology

Figure 3 illustrates the simulated network. Two end nodes are connected with each other via the base station that monitors every packet that passes through the connection in both directions. The network model consists of a 10 Mbps, 20ms delay wired channel and a 2Mbps wireless channel with 10ms delay.

In experimentation of this paper, TCP or SCTP agent exists at each edge nodes. We assumed that all packet losses are occurred in wireless network. So, error model of simulation is simplified and only considered transmission error of wireless networks. In all the simulation runs, there are 1000byte data segments transferred (excluding headers) for TCP and 1000byte data chunks (excluding headers) for SCTP.

We used the total time to transfer data for performance evaluation. We measured the performance using ftp application which transfers data from 1Mbyte to 10Mbyte.

4.2 SCTP vs TCP

We first ran a test to compare the performance of original SCTP with that of original TCP under same loss over wireless networks.

Figure 4 shows that the total time of original SCTP to transfer files are almost half of one of original TCP.

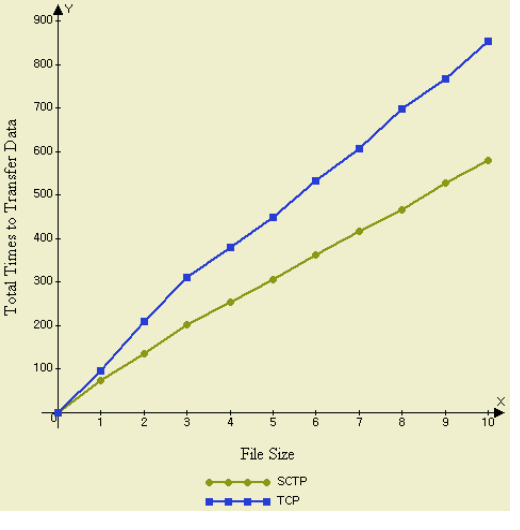

Fig. 4. SCTP vs TCP

Both original TCP and SCTP transfer data through wireless network with packet loss. If packet losses occurred in wireless networks, source node could regard it as congestion by packet loss of wireless network. So, both TCP and SCTP have executed congestion control in order to recover packet losses. This is affected by congestion control.

Therefore, the result of this experimentation can be explained that SCTP uses more enhanced congestion control than TCP.

4.3 SCTP vs TCP Snoop

In the second simulation, we have compared original SCTP with TCP Snoop. As shown in the figure 5, the total time of SCTP to transfer data has been delayed more than TCP Snoop.

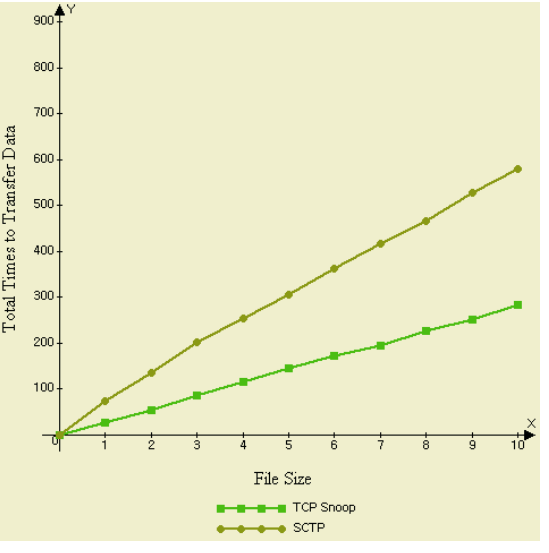

Fig. 5. SCTP vs TCP Snoop

TCP Snoop agent immediately doesn't deliver information about packet loss which occurred in wireless networks to the fixed host at wired networks, but Snoop agent processes packet loss using the buffer which stores packet received from the sender, thereby avoiding unnecessary fast retransmissions and congestion control invocations by the sender.

So, TCP Snoop achieved performance enhancement more than original TCP. But SCTP doesn't use the performance enhancement protocol such as Snoop Protocol of TCP.

If SCTP receives a duplicate acknowledgement and transmission error by retransmission timeout, SCTP regards it as packet loss. At this time, the performance of the network has fallen by congestion control. Therefore, SCTP will need SCTP Snoop like TCP Snoop for performance enhancement in wireless networks.

4.4 SCTP Snoop vs Original SCTP and TCP Snoop

In this paper, we used modified Snoop Protocol for SCTP because Snoop was TCP-aware protocol. Figure 6 shows the total time to transfer data of SCTP Snoop and TCP Snoop. As shown in the figure, the total time of SCTP Snoop is the shortest among TCP Snoop and Original SCTP.

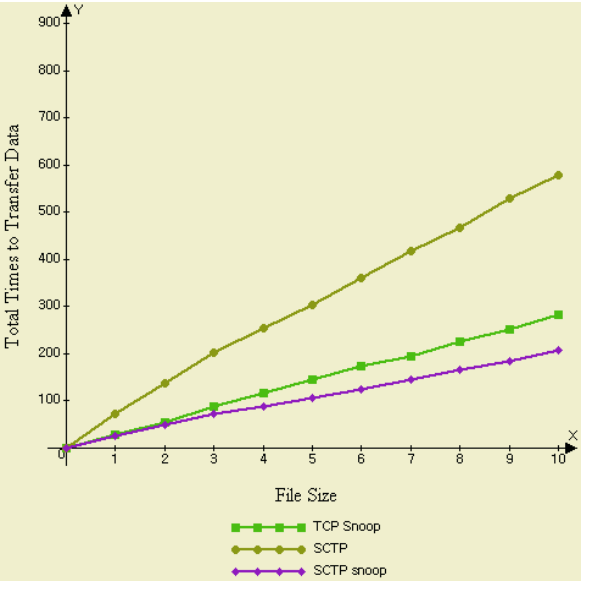

Fig. 6. SCTP-Snoop vs SCTP,TCP Snoop

Like TCP-Snoop, SCTP-Snoop hides the packet loss from the fixed host, thereby preventing unnecessary congestion control mechanism invocations.

The result of this experimentation can be explained that SCTP Snoop has achieved performance enhancement more than original SCTP just as TCP Snoop has achieved performance enhancement of TCP in wireless networks.

4.5 The Number of Packets

One of the main reasons that the preceding chunk-based format was chosen for SCTP was its extensibility.

SCTP and TCP header are slightly different [1]. SCTP packets are made up of an SCTP common header and specific building blocks called chunks. The SCTP common header provides SCTP with specific validation and associative properties. Chunks provide SCTP with the basic structure needed to carry information. Also, each chunk has header of its own in order to provide various information such as chunk type, TSN.

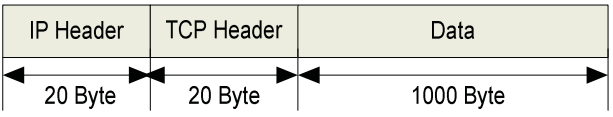

Fig. 7. TCP Packet Format

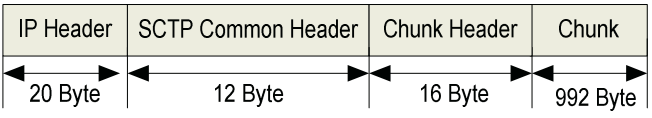

Fig. 8. SCTP Packet Format

Figure 7 and Figure 8 are packet formats used in our experimentations. We used SCTP packet of 1040byte size same as TCP packet. As in this figures, we ascertained the facts that SCTP has header size bigger 8byte than TCP. So, SCTP sends more packets than TCP with the same packet size.

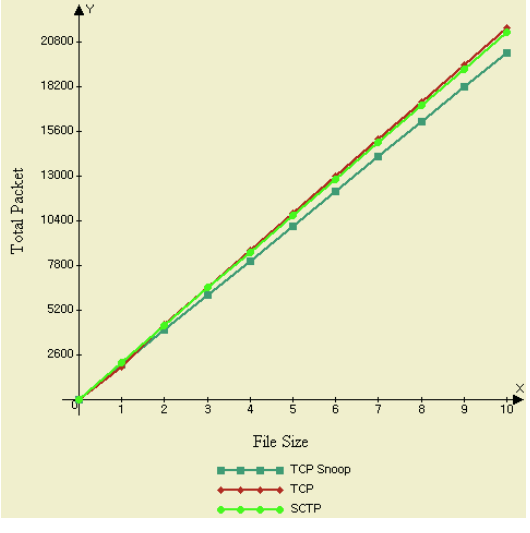

Fig. 9. The number of Packets comparison of SCTP and TCP

SCTP has a multi-homing feature. To support it, SCTP uses the HEARBEAT chunk type of 56byte. It is used to periodically probe reachability of the destination addresses and update the RTT of a destination address. So, the transmission of the HEARBEAT chunk is one of the reasons increasing total packet counts of SCTP.

Through figure 9, we show that SCTP interchanges more packets than TCP Snoop during the data transmission. The increase of packet counts not only cause more congestion control by packet loss in wireless networks, but also degrade the performance due to overload when many users use wireless networks with low bandwidth and high delay.

5 Conclusion and Future Work

We carried out 3 experimentations over wireless networks with packet loss as following: at first experimentation, we compared the performance of TCP with SCTP by sending 10 different file size. It showed the total time of SCTP to transfer files is almost half of one of TCP. We believe that original SCTP uses more enhanced congestion control than original TCP in wireless networks. Since our experiment environment has some packet loss, its congestion control scheme is effective. At second experimentations, we compared the performance of TCP-snoop with SCTP. It showed that original SCTP has less performance than TCP Snoop in wireless networks. The reason for this would be that TCP-snoop helps TCP engine to avoid unnecessary congestion control process which severely affects delay. At third experimentations, the performance of the proposed SCTP-Snoop was compared with original SCTP. We found that the performance of SCTP-Snoop in wireless network was improved over original SCTP and TCP-Snoop.

We have shown that SCTP sent more packets than TCP. It can be one of reasons of SCTP performance degradation because the increasing of packet counts have influence on the more congestion control execution and it can occur overload by sharing in wireless networks by many users.

In this research, we modified SCTP by including Snoop mechanism properly. We show that SCTP-snoop approach is effective over wireless networks.

For the future work, we want to find the sources of performance degradation thru continuous experimentations, and to improve SCTP protocol based on intrinsic SCTP features.

References

[1] 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" Proposed standard, RFC 2960, Internet Engineering Task Force(IETF),October 2000.

[2] R. Stewart, Qiaobing Xie, "Stream Control Transmission Protocol:a reference guide", Addison-Wesley 2001.

[3] G. Xylomenos, G. C. Polyzos, P. Mahonen and M.Saaranen, "TCP Performance Issues over Wireless Link ", IEEE Communications Vol. 39 No.4 pp.52-58, April 2001.

[4] Hari Balakrishnan, Srinivasan Seshan, Elan Amir, Randy H. Katz. "Improving TCP/IP Performance over Wireless Networks ", Proc. 1st ACM Conf. on Mobile Computing and Networking, Berkeley, CA, November 1995.

[5] R. Brennan and T. Curran, "SCTP congestion control : Initial simulation studies", International Teletraffic Congress(ITC 17), Brazil, 2001

[6] UC Bekely, LBL, USC/ISI, and Xerox Parc. Ns-2 documentation and software, Version 2.7, January 2004. http://www.isi. edu/nsnam/ns/index.html

[7] A. Caro and J. Iyengar. Ns-2 SCTP module, Version 3.4, August 2003. http://pel. cis.udel.edu