Advanced Communication Protocol Technologies:

Solutions, Methods, and Applications

Katalin Tarnay
University of Pannonia, Hungary

Gusztáv Adamis
Budapest University of Technology and Economics, Hungary

Tibor Dulai
University of Pannonia, Hungary

Information Science
REFERENCE

Senior Editorial Director:	Kristin Klinger
Director of Book Publications:	Julia Mosemann
Editorial Director:	Lindsay Johnston
Acquisitions Editor:	Erika Carter
Development Editor:	Hannah Abelbeck
Production Editor:	Sean Woznicki
Typesetters:	Mike Brehm, Keith Glazewski, Natalie Pronio, Jennifer Romanchak, & Deanna Zombro
Print Coordinator:	Jamie Snavely
Cover Design:	Nick Newcomer

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data
Advanced communication protocol technologies : solutions, methods, and applications / Katalin Tarnay, Gusztáv Adamis, Tibor Dulai, editors.
p. cm.
Includes bibliographical references and index.
Summary: "This book explores the complications and solutions created by communication required between ever-expanding technologies, covering the fundamentals of protocol functions and protocol operations, the controlling protocols of ISDN and mobile networks, the evolution of IP-based protocols, and advanced solutions for routing, mobility and multimedia transmission"-- Provided by publisher.
ISBN 978-1-60960-732-6 (hardcover) -- ISBN 978-1-60960-733-3 (ebook) -- ISBN 978-1-60960-734-0 (print & perpetual access) 1. Telecommunication. I. Tarnay, Katalin. II. Adamis, Gusztáv, 1965- III. Dulai, Tibor, 1979-
TK5101.A35 2011
621.382'12--dc23
2011013392

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 18
SCTP:
Solution for Transport Layer Mobility and Multihoming

Árpád Huszák
Budapest University of Technology and Economics, Hungary

Sándor Imre
Budapest University of Technology and Economics, Hungary

ABSTRACT

Numerous protocols were introduced in the transport layer, which can be very different depending on the provided services. Beside the traditional TCP and UDP, new transport protocols (SCTP, DCCP) have appeared in recent years to overcome limitations of the conventional protocols. The unique features of SCTP like multihoming and multistreaming make this protocol very attractive for reliable data delivery of streams, even in a mobile environment. It can be also used for applications where monitoring and detection of loss is required. SCTP is the only transport protocol that is able to manage mobility issues and handle handovers in the transport layer. The multihoming feature allows an endpoint of a SCTP association to be mapped to multiple IP addresses, and change the delivery path according to the link conditions. The handover process is hardly influenced by several protocol parameters that can be adjusted by the user. The effects of different protocol settings are investigated in details in this chapter. We have studied the performance of multihomed SCTP hosts through experimental studies in an integrated heterogeneous environment. SCTP will also play a significant role in future LTE–EPS architecture, because it can also be used for core network signaling purposes, not just for user data delivery.

DOI: 10.4018/978-1-60960-732-6.ch018

INTRODUCTION

The transport layer is essential part of the ISO/OSI reference model, as well the TCP/IP protocol stack. Different transport layer protocols were already introduced, which can be very diverse depending on the provided services. The responsibilities of the transport protocols include end-to-end message transfer capabilities independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers). In order to select the most appropriate protocol to effectively fulfill the users' requirements, the properties and characteristics of the different transport protocols must be studied. For delay sensitive multimedia applications simple and fast protocols are recommended, while for reliable data transfer the information must be delivered ordered and without any error.

In the next-generation mobile network, the need for mobility management even in the transport layer has been revealed. Mobility is becoming increasingly popular feature for the Internet users; however, the developers of the early network protocols did not take into consideration this possibility. For the next-generation Internet, one of the most essential requirements is to make the roaming possible without loosing the connection between the corresponding hosts. Anywhere, anytime communications is an indispensable need in the future networks. Moreover, with the extensive growth of the Internet and mobile/wireless systems, the user demand for high-speed data access caused the introduction of many different kinds of access technologies. Therefore, future telecommunication architectures could easily appear as an integration of multiple wireless access technologies (e.g. Bluetooth, UMTS, WLAN, WiMAX, etc.). Mobile hosts equipped with multiple network interfaces can be connected to the Internet via different ISPs. Failures in one network cannot easily break ongoing communication sessions if hosts are capable of switching over to another connection. Moreover, if both connections are active at once, but higher packet loss and delay is experienced on one path, multihoming capabilities can be used to hand over current sessions to the connection offering better values of Quality of Service (QoS) parameters.

Mobility and multihoming support can be provided in different layers of the ISO/OSI architecture (Ratola, M., 2004; Eddy, W. M., 2004). Mobile IP (Johnson, D & Perkins, C. & Arkko, J., 2004) with Multiple Care-of Addresses (MCoA) (R. Wakikawa et al., 2007) extension is a layer 3 solution, while several proposals exist also in the transport (Stewart, R., 2007) and even in the application layer (Rosenberg, J et al., 2002). Novel solutions for mobility handling based on HIP (Host Identity Protocol) were also appeared in the recent years (Bokor, L. et al., 2007; Bokor, L., et al, 2009).

In this chapter, we introduce SCTP and its unique multihoming and multistreaming features implemented in the transport layer. The most well known transport protocols are the TCP (Transmission Control Protocol) (Postel, J., 1981) and UDP (User Datagram Protocol) (Postel, J., 1980) standardized in the early years of the Internet age. In the last decade, new protocols were investigated with enhanced features. SCTP is one of these protocols, which uniquely provides multihoming and multistreaming. With multihoming capabilities, SCTP is the only transport layer protocol, which can be utilized in mobile networks, where the hosts are continuously changing their access points to the network.

In this chapter, we focus on SCTP and its multihoming and multistreaming performance over heterogeneous IP networks. We used a native IPv6 UMTS–WLAN environment to analyze the behavior of the protocol from mobility point of view. Building our SCTP testbed based on a native IPv6 architecture resides in the fact that IP is considered as the best solution to integrate heterogeneous wireless access networks, and IPv6 will actually be the main networking protocol of the next generation Internet. In order to study multihoming in an integrated, all-IP heterogeneous mobile environment, we realized a native IPv6 UMTS–WLAN testbed and examined the main performance measures of an SCTP-based Layer 4 mobility/multihoming architecture. Besides the empirical results of the SCTP mobility handling performance, we also made analytical models to estimate the handover process efficiency.

SCTP can be used in the core network for signaling purposes, too. In a GSM, 3G UMTS, or 4G networks, the MSC (Mobile Switching Centre) may connect to other SSPs (Service Switching Point), STPs (Service Transfer Point), or SCPs (Service Control Point) via a traditional SS7 protocol stack or via SIGTRAN (Signaling Transport). SIGTRAN consists of three components: a standard IP layer, an SCTP layer, and user adaptation layers. The Evolved Packet Core (EPC) is the mobility core solution associated with the Evolved Universal Terrestrial Radio Access Network (E-UTRAN), which was formally known as Long Term Evolution (LTE). EPC and E-UTRAN are defined by 3GPP's Release 8 specifications. The combination of E-UTRAN and EPC is called Evolved Packet System (EPS). In the EPS, SCTP is used over the usual IP network layer in order to provide reliable and efficient transport between the e-NodeB and the MME (Mobility Management Entity) core entities. Based on the SCTP's multistreaming capabilities, all dedicated EPS procedures, which include all functions, which apply to a specific communication context, can be supported over a limited number of SCTP streams and with improved transmission efficiency. In this chapter, we introduce the role of SCTP in future LTE–EPS architectures, too.

BACKGROUND

In the early years of the Internet era, two transport protocols were introduced for wired network communication. The first one is the UDP (User Datagram Protocol) (Postel, J., 1980), which uses a simple transmission model without handshaking connection setup, reliability, ordering, or data integrity. The other well-known transport protocol is the TCP (Transmission Control Protocol) (Postel, J., 1981), which a more complex protocol offering reliable, connection oriented and ordered delivery of data. Other important features of TCP are flow control, retransmission of lost data and congestion avoidance. New transport protocols (DCCP, UDPLite, and SCTP) appeared in the recent years to overcome the limitations of the traditional protocols. The DCCP (Datagram Congestion Control Protocol) (Kohler, E. & Handley, M. & Floyd, S., 2006) is a newly defined transport protocol by the IETF that implements bidirectional, unicast connections of congestion controlled, unreliable datagrams. For real-time applications the time constraints are more important than reliability, so media transmissions typically use transport protocols like UDP, where no retransmission occurs, providing minimal packet delay. Presently the reliable TCP, SCTP, and the unreliable DCCP are the only alternative protocols to provide congestion control. DCCP combines the best features of UDP and TCP protocols within media transmission context, supporting congestion control mechanisms. It may be useful to think of DCCP as TCP minus bytestream semantics and reliability, or as UDP plus congestion control, handshakes, and acknowledgements. DCCP, similarly to UDPLite (Larzon et al., 2004), is designed to provide a partial checksum that only covers as much of the user data that the sending application specifies in the DCCP Generic Header. Errors in the rest of the packet are ignored because they are assumed acceptable for the destination application. DCCP connections are congestion controlled, but unlike in TCP, DCCP applications have a choice of congestion control mechanism. DCCP uses Congestion Control Identifiers (CCID) to determine the congestion control mechanism. Currently two identifiers are being defined: CCID2 that implements a TCP-like Congestion Control and CCID3 that implements a TCP-Friendly Rate

Control (TFRC), but DCCP is easily extensible to further forms of unicast congestion control.

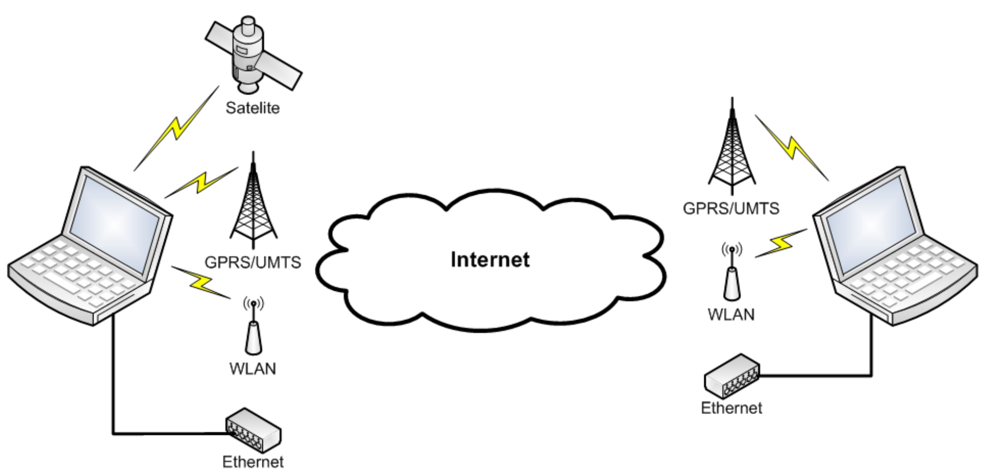
Other alternative for end-to-end, real-time, transfer of multimedia data is RTP (Real-time Transport Protocol) (Schulzrinne, H. et al., 2003). The protocol provides facility for jitter compensation and detection of out of sequence arrival in data that are common during transmissions on an IP network. RTP typically use UDP, but may use other transport protocols (most notably, SCTP and DCCP) as well, as the protocol design is transport independent.

Recent applications running on mobile hosts may found TCP too limiting due to disconnections during handovers and parallel connections to the same corresponding node. Some applications need reliable transfer without sequence maintenance (e.g. transmission of control data), while others may process received packets strict sequence order (e.g. file downloading). In both of these cases, the head-of-line blocking causes unnecessary delay if TCP is used. The stream-oriented nature of TCP is often an inconvenience, because applications must add their own record marking to delineate their messages. Developers of SCTP were motivated to fulfill the needs of these applications.

New mobile equipments integrate several access technologies to make connections possible to different type of networks. Simultaneous usage of these interfaces may increase bandwidth availability or to select the most appropriate access technology according to the type of flow or choices of the user. A multihomed endpoint determinates a host with several network interfaces. To manage these interfaces, a novel feature, called multihoming support must be introduced to efficiently control these interfaces for improved connectivity (See Figure 1).

In order to increase the reliability of the end-to-end connection, multihoming is an advantageous technique, because it makes possible to reach the multihomed host on more then one IP address. The traffic from one node to another may be forwarded on physically different paths (different subnetworks and thus different destination IP addresses are used) by configuring the communicating endpoints and the IP network accordingly. In this case, associations may become tolerant against physical network failures. When one of the interfaces/paths becomes unavailable, the other paths are still ready to deliver data. Besides, multi-access provides ubiquitous access to offer an extended coverage area for the mobile hosts. It is also a good opportunity to spread network traffic load among several routes, and distribute traffic load among different connections.

Figure 1. Multihomed hosts



For the efficient interface management of a multihomed host, the corresponding paths must be monitored continuously. When the condition of the actual interface/path is getting worse or fail, a new interface should be assigned for the connection immediately. One of the most important issues is to change the primary path seamlessly; therefore, the endpoint must recognize the link failures as soon as possible and change the active IP address corresponding to a reachable path. However, instantaneous delay increase or temporal channel errors should not cause the change of the primary path. The IP change trigger may depend on several link parameters and protocol settings. It must be defined in the protocol settings, when should a path considered broken and change to another path. The number of retransmission attempts, the packet loss ratio and different time constrains may affect the performance of the interface/path changes.

Alternative Multihoming Solutions

Besides SCTP, other alternative solutions also exist. Based on the IPv6 protocol different approaches have been appeared.

The simplest solution is named *host multihoming*, where the host can have multiple global addresses, one assigned for each of the site's upstream providers with different IP addresses on each interface. While the host knows its addresses, it can choose which source address to use. Multihoming is managed by the application.

The other IPv6-based solution is *site multihoming*, where a host is unaware it is multihomed, allowing the site gateway routers to handle to multiple routing. Site Multihoming by IPv6 Intermediation (SHIMP6) (Nordmark & Bagnulo, 2009) specifies a network layer approach and protocol for providing locator agility below the transport protocols. Multihoming can be provided for IPv6 with failover and load spreading properties, without assuming that a multihomed site will have a provider independent IPv6 address prefix, which is announced in the global IPv6 routing table. The SHIM6 protocol stack uses constant endpoint identities to refer to both itself and to the remote protocol stack. The SHIM6 layer provides a set of associations between endpoint identity pairs and locator sets. The hosts in a site that has multiple provider-allocated IPv6 address prefixes can use the SHIM6 protocol to set up state with peer hosts so that the state can later be used to failover to a different locator pair in case of link errors.

IP addresses can serve only as short term identifiers, because a considerable amount of hosts are portable devices and they change their IP addresses when moved from one network to another. Short-term identifiers disrupt long-term transport layer connections, such as VoIP phone calls, and make locating the peer host more difficult. Therefore, mobility and multihoming are hard to implement securely in the present Internet. Host Identity Protocol uses Host Identifier, to mark uniquely all the hosts which connect to the Internet. The Host Identifier is global unique. The main purpose is to disconnect the close connection between network layer and transport layer so that the function of IP will be concentrated on IP routing. The mark of service in the upper layer will rely on HIP layer.

SCTP

SCTP (Stream Control Transmission Protocol) is a general-purpose transport protocol for the Internet. It was defined by the IETF Signaling Transport (SIGTRAN) working group and described in RFC 4960 in year 2000. SCTP is new protocol operating on top of a connectionless packet network such as IP. Similarly to TCP (Transmission Control Protocol), it also provides connection oriented, reliable and ordered delivery of data between two endpoints.

The developers of SCTP aimed to create a transport protocol that would overcome the limitations of TCP and UDP. SCTP offers the following services to its users:

- acknowledged error-free, non-duplicated transfer of datagrams
- data fragmentation to conform to discovered path MTU size
- multistreaming: sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages
- optional bundling of multiple user messages into a single SCTP packet
- multihoming: network-level fault tolerance through supporting of multihoming at either or both ends of an association.

Detection of data to provide reliability, a selective retransmission mechanism is applied. SCTP can also be used for applications where monitoring and detection of loss is required. For such applications, the SCTP failure detection mechanisms will actively monitor the session. These mechanisms are also used to manage the SCTP handover process in case of multihomed hosts.

The used end-to-end window based flow- and congestion control mechanisms in SCTP are similar to the one that is used in TCP. SCTP also uses an Additive Increase, Multiplicative Decrease (AIMD) algorithm, but the congestion control mechanism of SCTP has been modified and adapted for multihoming. SCTP endpoints may be reachable by more than one transport address through different data paths. For each possible path a discrete set of flow and congestion control parameters are maintained. The major feature that confers a distinction on SCTP is that SCTP provides multihoming and multistreaming. The multihoming feature enables to be used for mobility support, without any special router agents or anchor points in the network, while multistreaming supports multiple independent streams within an association. SCTP has several features that are unique, like multistreaming and multihoming.

The comparison of SCTP and other transport layer protocols are summarized in Table 1.

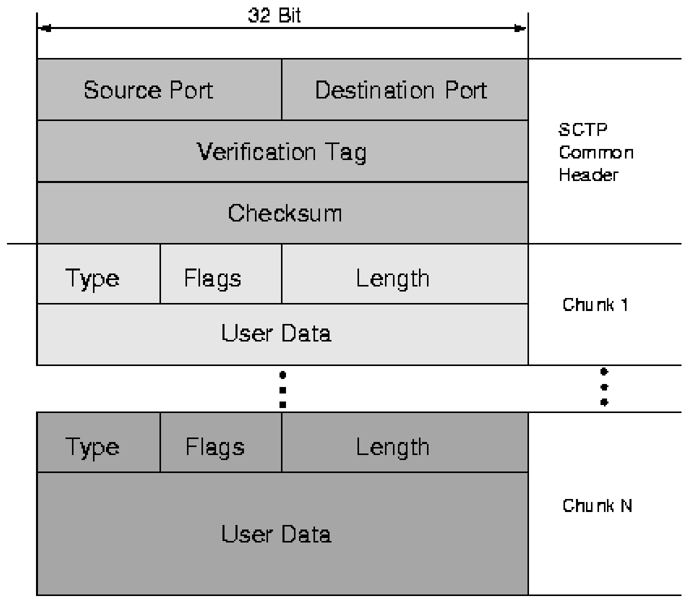
SCTP packets have a simpler basic structure than TCP packets. An SCTP packet is composed of a common header, which occupies the first 12 bytes and chunks. A chunk contains either control information or user data. The SCTP packet format is shown in Figure 2.

Similarly, to other transport protocols, the port numbers identify the association to which this packet belongs. The Verification Tag is used to

Table 1. Comparison of transport protocols

Feature	SCTP	TCP	UDP	UDP Lite	DCCP
Connection oriented	yes	yes	no	no	yes
Reliable	yes	yes	no	no	no
Ordered delivery	yes/no	yes	no	no	no
Checksum	yes	yes	yes	yes	yes
Checksum size (bits)	32	16	16	16	16
Partial checksum	no	no	no	yes	yes
Path MTU	yes	yes	no	no	yes
Congestion control	yes	yes	no	no	yes
Flow control	yes	yes	no	no	yes
Multistreaming	yes	no	no	no	no
Multihoming	yes	no	no	no	no

Figure 2. SCTP header



validate the sender of this SCTP packet. The chunk begins with a chunk type field, which is used to distinguish data chunks and different types of control chunks. Multiple chunks can be bundled into one SCTP packet up to the MTU size, except for some special chunk types for initialization and shutdown. The defined chunk types are presented in Table 2.

Security considerations were also important for the SCTP investigators. The protocol was designed with features for improved security, such as 4-way handshake (TCP uses 3-way handshake) to prevent against SYN-flooding attacks.

One of the key aspects was reliability that is also strengthened with the multihoming feature. Multihoming enables an SCTP association to stay open even when some links and interfaces are down. This feature is particularly important for SIGTRAN; because it carries SS7 over TCP/IP network using SCTP, and requires strong resilience during link outages to maintain telecommunication service even when enduring network anomalies.

From mobility point of view, multihoming is the most important feature of the SCTP protocol, while other unique feature is multistreaming. Both of these elements are introduced in details in the following subsections.

Multistreaming in SCTP

SCTP makes it possible to deliver independent streams within one association. Each stream has a stream number that is included inside SCTP packets' chunk headers. Multistreaming eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery. On the receiving side, SCTP ensures that messages are delivered to the SCTP user in sequence within a given stream. However, while one stream may be blocked waiting for the next sequence user message, delivery from other streams may proceed. User messages sent in independent streams are delivered to the SCTP user as soon as they are received. In other words, a blocked stream does not affect the other streams in an association.

Multiple data and control chunks may be bundled by the sender into a single SCTP packet for transmission, as long as the final size of the

Table 2. SCTP chunk types

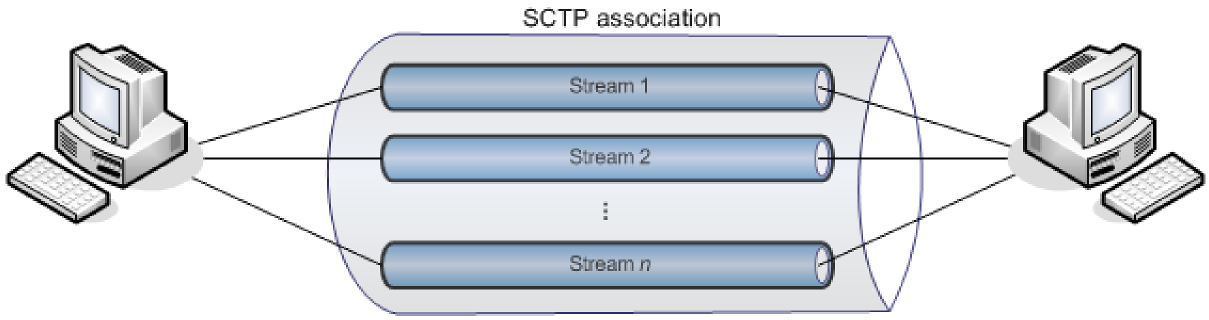
Chunk type	Description
Payload Data (DATA)	Used for data transfer.
Initiation (INIT)	Initiates an SCTP association between two endpoints.
Initiation Acknowledgement (INIT ACK)	Acknowledges the receipt of an INIT chunk. The receipt of the INIT ACK chunk establishes an association.
Selective Acknowledgement (SACK)	Acknowledges the receipt of the DATA chunks and also reports gaps in the data.
Cookie Echo (COOKIE ECHO)	Used during the initiation process. The endpoint initiating the association sends the COOKIE ECHO chunk to the peer endpoint.
Cookie Acknowledgement (COOKIE ACK)	Acknowledges the receipt of the COOKIE ECHO chunk. The COOKIE ACK chunk must take precedence over any DATA chunk or SACK chunk sent in the association. The COOKIE ACK chunk can be bundled with DATA chunks or SACK chunks
Heartbeat Request (HEARTBEAT)	Tests the connectivity of a specific destination address in the association.
Heartbeat Acknowledgement (HEARTBEAT ACK)	Acknowledges the receipt of the HEARTBEAT chunk.
Abort Association (ABORT)	Informs the peer endpoint to close the association. The ABORT chunk also informs the receiver of the reason for aborting the association.
Operation Error (ERROR)	Reports error conditions. The ERROR chunk contains parameters that determine the type of error.
Address Configuration Change Chunk (ASCONF)	Request configuration changes.
Address Configuration Acknowledgment Chunk (ASCONF-ACK)	Configuration changes must be acknowledged.
Shutdown Association (SHUTDOWN)	Triggers a graceful shutdown of an association with a peer endpoint.
Shutdown Acknowledgement (SHUTDOWN ACK)	Acknowledges the receipt of the SHUTDOWN chunk at the end of the shutdown process.
Shutdown Complete (SHUTDOWN COMPLETE)	Concludes the shutdown procedure.

packet does not exceed the current path MTU. The receiver will unbundle the packet back into the original chunks. The application may also request a stream to be delivered unordered, which can reduce blocking effects in case of message loss, since the reordering mechanism of one stream is not affected by another stream. SCTP multistreaming is particularly effective in cases, when independent control and data channels are considered in the communication. In TCP, control and data typically share the same connection, which can be problematic, because control packets can be delayed behind data packets. If control and data messages are delivered within independent streams, control data could be dealt with in a timelier manner, resulting better utilization (See Figure 3).

Multihoming in SCTP

Besides multistreaming, the other most important enhancements in SCTP over traditional transport layer protocols is the multihoming capability. A multihomed SCTP endpoint is represented to its peers as a combination of a set of eligible destination transport addresses to which SCTP packets can be sent and a set of eligible source transport addresses from which SCTP packets can be received. A multihomed host can be reached using more than one IP addresses, usually through more than one network interfaces. This feature allows an endpoint of a SCTP association to be mapped to multiple IP addresses. One of the possible IP addresses is selected as Primary Address, while the Primary Path is considered as the network

Figure 3. Multiple streams within one SCTP association



path that leads to the Primary Address. Unless specified otherwise by the SCTP user, an endpoint should always transmit on the Primary Path. The sender may change the Primary Address if the number of failures on the Primary Path exceeds a certain threshold. Retransmissions should be done on different paths as well, so when one link is overloaded, retransmissions do not affect it.

SCTP was developed to take full advantage of such a multihomed host to provide a fast failover and association survivability in the face of such hardware failures. In order to provide fast failover all the available addresses must be bound to the association. While mobile host are able to change the IP address of an interface due to mobility management of the network layer protocol, the SCTP must dynamically add the new IP address to the association. The dynamic addition and subtraction of IP addresses allows an SCTP association to continue to function through host and network reconfigurations. These changes, brought on by provider or user action, may mean that the peer would be better served by using the newly added address; however, this information may only be known by the endpoint that had the reconfiguration occur. If a client is multihomed, it informs the server about all its IP addresses with the INIT chunk's address parameters during the 4-way handshake connection setup. Hence, the client is required to know only one IP address of the server, because the server provides all its IP addresses to the client in the INIT-ACK chunk. After the connection setup a new addresses can be added or removed within an ASCONF chunk. The implementations of Linux 2.6.x versions of SCTP are able to handle both IPv4 and IPv6 addresses. There are numerous protocol parameters (heartbeat interval, retransmission timeout, path maximum retransmission, etc.) that can be adjusted by the user in order to change the SCTP behavior during failovers/handovers. In Linux/BSD operation systems, the *sysctl* is used to modify kernel parameters at runtime. *Sysctl* is an interface for examining and dynamically changing parameters in Linux or BSD.

An SCTP instance monitors all transmission paths to the peer instance of an association. An important feature of the SCTP regarding multihoming is the heartbeat mechanism, which detects failures in idle paths and endpoints. The aim of this mechanism is to detect whether a destination address is active or passive. HEARTBEAT chunks are sent periodically to all idle destinations, and the number of sent HEARTBEAT messages without receipt of a corresponding HEARTBEAT-ACK is maintained. The timing of the HEARTBEAT chunks for destination i is determined by the *HB.Interval* and *RTO* (Retransmission Timeout) protocol parameters according to the following equation:

$$H_i = RTO_i + HB.Interval(1 + \delta) \tag{1}$$

where δ is a random value between -0.5 and 0.5 and *RTO* is the Retransmission Timeout for path *i*.

An address or path is considered active if acknowledgement is received from its peer within a defined time period (*RTO*). In this way *RTO* is a prediction of the upper limit of *RTT* (Round Trip Time). Separate *RTO* is maintained for each path, which is calculated using the smoothed average of the periodically measured RTT (*SRTT*) and the RTT variation (*RTTVAR*). From these, *RTO* is computed as

$$RTO = SRTT + 4RTTVAR \tag{2}$$

The address with the corresponding path is inactive if the number of consecutive transmission timeouts exceeds the Path Maximum Retransmission (*PMR*) protocol parameter. Every time when timeout occurs, the *PMR* counter is incremented and the value of the *RTO* is doubled for that path. If the new *RTO* is less than *RTO.Min*, it will be set to *RTO.Min*, if it is greater than *RTO.Max*, it will be set to *RTO.Max*. According to the previously presented procedure, the delay of the path failure recovery and the handover process can be calculated as follows:

$$\Delta = \sum_{i=0}^{PMR-1} 2^i \cdot RTO \tag{3}$$

In mobile environment where handovers may frequently occur, the failover time using default SCTP settings is likely to be unacceptable to users. Shortening the failover time can be achieved by setting the relevant protocol parameters (e.g. *RTO.Min, RTO.Max, and PMR*) to smaller values. When the Primary Address becomes unreachable or the link conditions are not acceptable, alternative IP address should be used if the endpoint is multihomed. With the heartbeat mechanism, the SCTP knows which other addresses are active or not and thus, can avoid using another path that has a failure.

Regarding to SCTP, mobility means the ability to change the endpoints and IP addresses while keeping the end-to-end connection. The change of communication link should be done with minimal disruption to the data transmission in progress in order to provide seamless communication in a changing environment. The multiple interface concept can be utilized in dynamic mobile networks, in which e.g., the host terminal has only one interface but the connection is frequently changed. If the possible IP addresses are known, they can be bound even at connection setup. Using the early IP address bindings, the handovers can be handled in such way, but with the dynamical IP binding, the new addresses can be bound during the data transfer.

Configuring SCTP Parameters

SCTP has a large number of adjustable association and path parameters that can be modified using *setsockopt*() linux kernel function.

Previous works examining SCTP mobility and multihoming performance are mainly based on simulations (Jungmaier, A. et al., 2006) or using emulator tools to imitate the behavior of different type of networks (Österdahl, H., 2005). Some of the first previous works dealing with SCTP mobility and multihoming performance evaluation in real life testbeds were (Ravier, T. et al., 2001) and (Jong-Shik Ha et al., 2005), where authors mainly confined their work to study how SCTP deals with packet loss and throughput in quite simple multihoming experiments. Authors of (Fallon, S. et al., 2008) examined SCTP switchover performance in a pure WLAN environment and showed that with the default parameters, SCTP implementations behave in a counterintuitive manner allowing more time for switchover when network conditions degrade. In addition, a pure WLAN testbed was used by authors of (Wakikawa, R. et al., 2006) in order to present a smooth handover scheme for Mobile IPv6 based on SCTP failover mechanism.

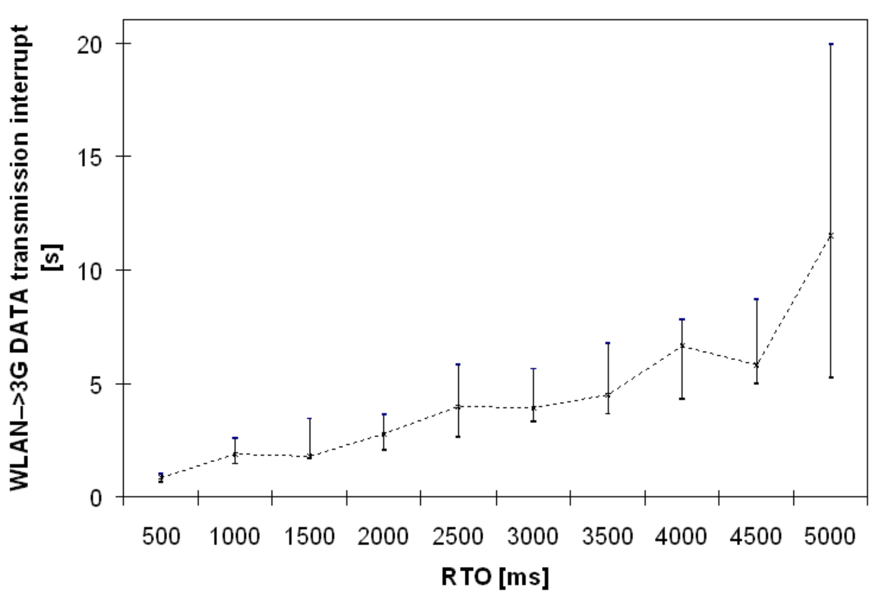
In order to increase the multihoming performance of the SCTP the endpoint must recognize the link failures as soon as possible and change the active IP address, but the handover delays or temporal channel errors should not cause the change of the primary path. The IP change trigger may depend on several protocol settings. It must be defined when should a path considered broken. The number of retransmission attempts, the packet loss ratio and different time constrains may affect the performance of the interface/path changes. From the handover point of view, the most important SCTP protocol parameters are *RTO.Min*, *RTO.Max,* and *Path.Max.Retransmission* (*PMR*). These parameters and the continuously calculated *RTO* value determinate the speed of the handover. By setting *RTO.Min* = *RTO.Max*, the *RTO* is kept on a constant value disabling to redouble it every time when timeout occurs, as equation (3) defines it. By adjusting these parameters, the handover process can be speed up. The delay of the path failure recovery and the handover process in this case can be calculated as follows:

$$\Delta = PMR \cdot RTO \tag{4}$$

To analyze the effect of *RTO* on the handover process we have measured the DATA transmission interrupt in our IPv6-capable UMTS–WLAN heterogeneous testbed. This interrupt is considered as the elapsed time between the last DATA chunk sent on the failed primary (WLAN) interface and the first DATA chunk arrived at the continuously available secondary (UMTS) interface. In order to seamlessly forward real-time data, the handover delay must be decreased, which highly depends on the current *RTO* (See Figure 4).

To analyze the exclusively the *RTO* parameter, all the other parameters were kept constant (*HB. Interval* = 10s, *PMR* = 5) in our examinations. According to our previous considerations, the delay was rising linearly when the *RTO* parameter was incremented. As the results show, the transmission interrupt was lower then 10s when the *RTO* was less then 5s. Using the default SCTP parameters (*RTO.Min* = 1s, *RTO.Max* = 60s) the delay would rise exponentially due to *RTO* re-

Figure 4. DATA transmission interrupt measurements (WLAN→3G UMTS handover)



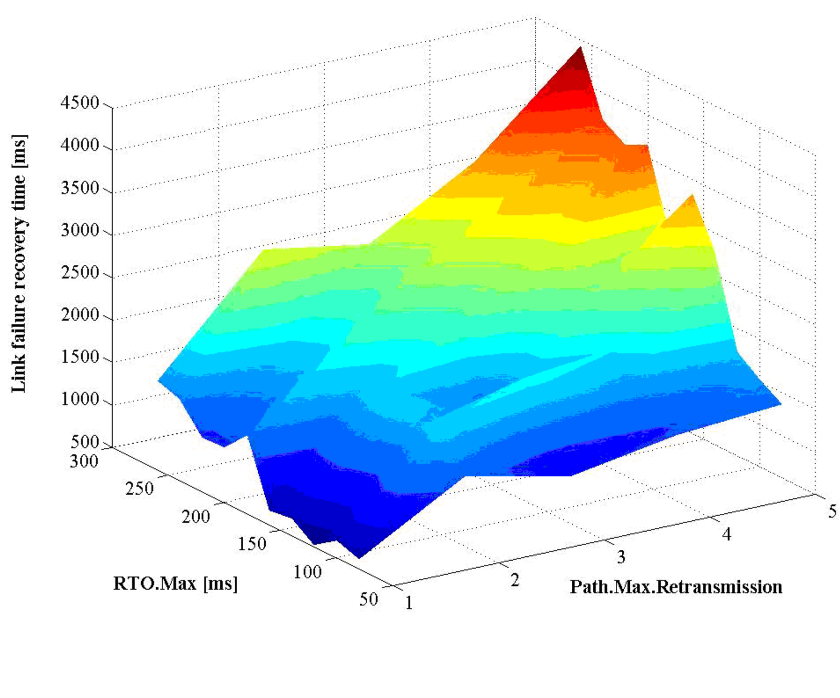
doubling and reach 60s. The average DATA transmission interrupt with default SCTP parameters was 227s, which is not acceptable for the users, especially for real time application users. If the *RTO* is forced to be less then 5s, the transmission delay can be significantly decreased.

The impact of *RTO* parameter is significant on the handover performance of SCTP, but the number of retransmission attempts on a link is also an important parameter. The *PMR* (Path Max. Retransmission) is the other key parameter of the SCTP handover. Parameter *PMR* contains the maximum number of retransmissions before the link shall be considered unreachable. Using the default parameters of the protocol, the link failure recovery time is rising exponentially according to equation (3). In the following figure, the joint impact of *RTO.Max* and *PMR* is introduced, based on our measurements in our native IPv6 UMTS–WLAN testbed (See Figure 5).

SCTP periodically sends HEARTBEAT chunks to idle destinations, or alternate addresses to identify a path failure. The heartbeat mechanism is also responsible for detecting when the primary path has recovered. The HEARTBEAT chunks are sent periodically as defined by the *HB.Interval* and the corresponding equation, see (1). SCTP maintains a counter to store the number of heartbeats that are sent to the inactive destination, without receiving a corresponding HEARTBEAT-ACK chunk. When the counter reaches the specified maximum value, SCTP also declares the destination address as inactive. SCTP notifies the application about the inactive destination address and starts using an alternate address for sending the DATA chunks. To discover that the primary path becomes available (link availability recognition time), it is desirable to keep the interval between HEARTBEATs relatively small. The obtained measurement results confirm this theory as Figure 6 shows.

SCTP continues to send HEARTBEATs to the inactive destination address until it receives a HEARTBEAT-ACK chunk. On receipt of the acknowledgement, SCTP considers the destination address as active again. When changing the com-

Figure 5. Link failure recovery time analysis in function of RTO and PMR (WLAN→3G UMTS handover)



munication path back to the primary path, the first packet on the primary link is always a HEARTBEAT chunk. The DATA chunk can be delivered only if HEARTBEAT-ACK is received. The primary link failure detection is independent from the *HB.Interval* parameter, while the recovery depends on it.

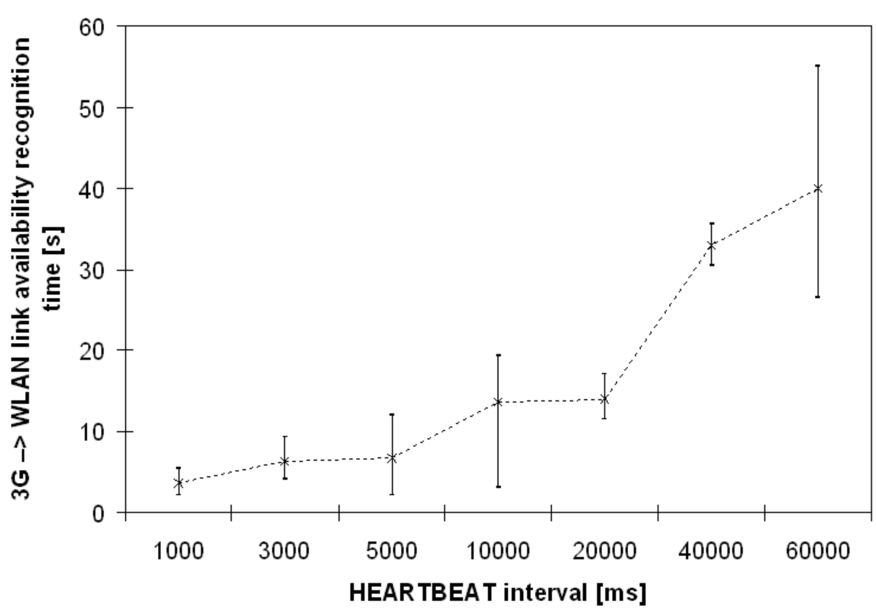
SCTP IN LTE NETWORKS

In mobile networks, the handovers cannot be avoided, but its negative effects can be minimized. SCTP multihoming and multstreaming feature can be effective in reducing of the disadvantages caused by handovers and lossy channels. The mobile terminal can switch between the base stations and between different access technologies (3G to WLAN, 3G to Ethernet, etc.) as well. The SCTP protocol can effectively reduce the handover delay and seamlessly continue the data delivery.

Stream Control Transmission Protocol was defined by the Signal Transport (SIGTRAN) working group of the Internet Engineering Task Force (IETF) and besides user data delivery, SCTP can be also used for signaling purposes. In a GSM, UMTS, or 4G network, the MSC (Mobile Switching Centre) may connect to other SSPs (Service Switching Point), STPs (Service Transfer Point), or SCPs (Service Control Point) via a traditional SS7 protocol stack or via SIGTRAN (Signaling Transport). SIGTRAN, as defined in RFC 2719 and RFC 4166, is a set of protocols that allow circuit-switched telephony messages, such as Media Gateway control and SS7 messages, to be reliably transported over an IP network. SIGTRAN consists of three components: a standard IP layer, an SCTP layer, and user adaptation layers.

The Evolved Packet Core (EPC) is the mobility core solution associated with the Evolved Universal Terrestrial Radio Access Network (E-UTRAN), which was formally known as Long Term Evolution (LTE). EPC and E-UTRAN are

Figure 6. The impact of the HEARTBEAT interval (HB.Interval) on the link availability recognition time (3G UMTS→WLAN handover)



defined by 3GPP's Release 8 specifications, in particular (3GPP TS 23.401, 2007; 3GPP TS 23.402, 2007; 3GPP TS 36.300, 2007). The combination of E-UTRAN and EPC is called Evolved Packet System (EPS) (See Figure 7).

In the EPS, SCTP is used over the usual IP network layer in order to provide reliable and efficient signal messaging between the e-NodeB and the MME (Mobility Management Entity) core entities. Based on the SCTP's multistreaming capabilities, all dedicated EPS procedures, which include all functions applying to a specific communication context, can be supported over a limited number of SCTP streams and with improved transmission efficiency. E-UTRAN introduces a new radio interface technology. A base station that supports this radio interface technology is called Evolved NodeB (e-NodeB). A logical interface (X2) is used to communicate between two e-NodeBs to deliver control information (See Figure 8).

The X2 signaling bearer provides the following functions, based on SCTP services:

- Provision of reliable transfer of X2-AP message over X2 interface.
- Provision of networking and routing function
- Provision of redundancy in the signaling network
- Support for flow control and overload protection

The S1 Application Part (S1-AP) is the control plane signaling protocol between the e-NodeB and the Mobility Management Entity (MME). LTE S1-AP implementation supports the S1-MME interface and utilizes SCTP in the transport layer. SCTP is for the control plane, which guarantees delivery of signaling messages between the MME and e-NodeB.

Unfortunately, SCTP may have negative features as well. With small-cell wireless deployments, the sheer number of SCTP connections that the EPC needs to manage has also increased. While the built-in reliability mechanisms of SCTP are attractive for providing carrier grade networks, they create substantial overhead. This behavior can lead to scalability problems in the EPC's core network.

Figure 7. LTE architecture

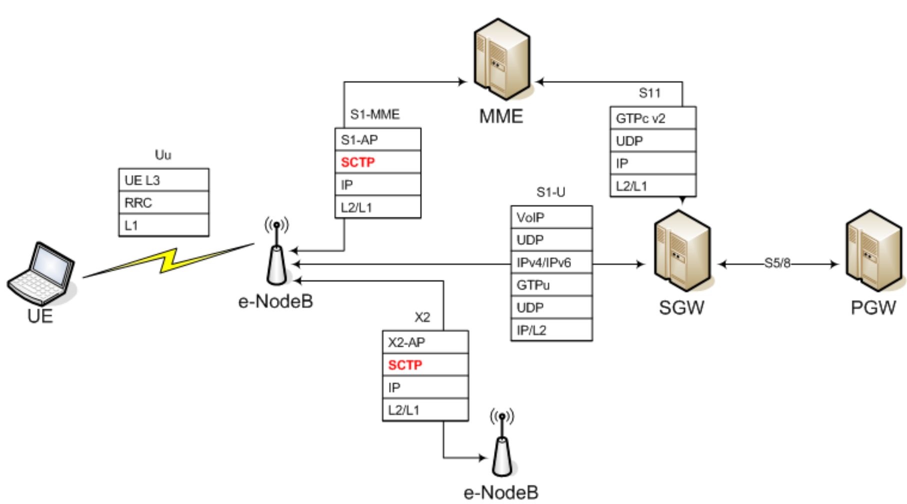
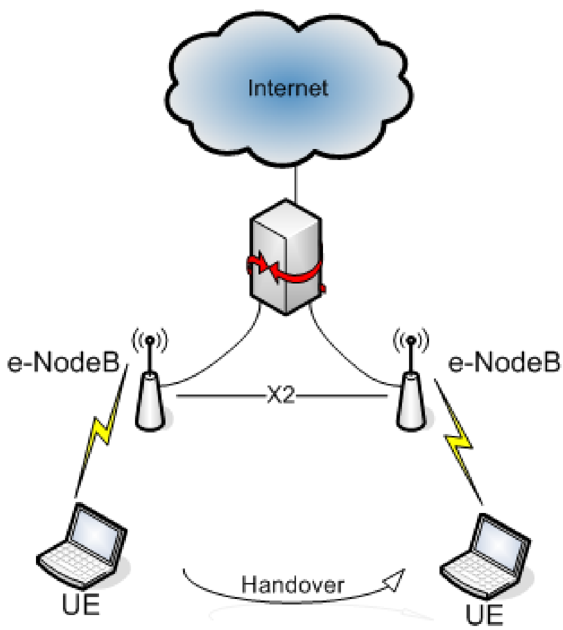


Figure 8. Logical interface (X2) between eNBs



SIP OVER SCTP

SCTP is the transport protocol specified by next generation network architectures and is used also by SIP, Diameter for AAA services, GCP-Gateway Control Protocol (H.248/MEGACO/MGCP), and SIGTRAN User Adaptation (UA) protocol layers. It provides secure and reliable transport, which is a must to fulfill the promise of next generation network services like multimedia messaging.

The use of SIP (Session Initiation Protocol) (Rosenberg, J., 2002) in the IP Multimedia Subsystem (IMS) requires servers that are capable to handle a large number of call requests. The signaling traffic associated to such requests could explode, if an intelligent congestion control were not introduced. SCTP as transport of SIP signaling might be useful in some situations, where usual transport protocols (e.g. TCP and UDP) suffer performance degradation. SIP itself is independent from the transport protocol, and can run over any reliable or unreliable message or stream oriented protocol.

If traffic is generated by a moderate number of sender-receivers sessions, no significant risk of congestion arises. In this case, UDP performs well, but as the number of sessions increases, the SIP retransmission mechanism increases the risk of causing a flood of retransmissions. In order to avoid the overload of the network, a transport protocol with congestion avoidance must be used.

A reliable transport layer as TCP guaranties the successful delivery, so retransmissions are not needed at an application level. However, TCP can cause the Head of Line (HOL) blocking problem when the signaling associated with multiple sessions is sent over a single TCP connection between two servers. The loss of one message stops the immediate delivery to the SIP layer of further messages; therefore, all other messages in the same flow, even if they belong to unrelated sessions, are affected by the loss of a message in a single session.

SCTP can overcome the problems of congestion and HOL. SIP transactions need to be mapped into SCTP streams to avoid HOL blocking. There are three possible ways to use SCTP with SIP:

- mapping of SIP sessions into Streams
- mapping of SIP transactions into Streams
- using Stream 0 and the unordered flag

It is important to note that most of the benefits of SCTP for SIP occur under loss conditions. Therefore, under a zero loss condition, SCTP transport of SIP should perform similarly to SIP/TCP transport.

CONCLUSION

In this chapter, we introduced the unique SCTP features, its utilization possibilities, and experimental analysis of SCTP in wireless environment in terms of handover effectiveness, throughput, and transmission delay. The multihoming behavior of SCTP is an advantageous feature of the protocol; however, its performance highly depends on the parameter settings. In our measurements, we have analyzed numerous settings to justify the analytical correlations of the protocol parameters and the different connection characteristics. Using accurate SCTP parameter setup, the handover delay, and the data transmission interrupt can be significantly decreased. SCTP will play important role in the future LTE networks as the transport layer protocol of signaling messages between the e-NodeBs and the Mobility Management Entity. Besides signaling purposes SCTP can also attractive as the transport protocol of SIP-based applications. Due to the special features of the SCTP protocol, it will become more and more popular in the IP-based networks.

ACKNOWLEDGMENT

This work was supported by the Mobile Innovation Center. The authors would like to express their appreciation to László Bokor and Gábor Jeney for their essential work on this research.

REFERENCES

Bokor, L., Nováczki, S., & Imre, S. (2007). *A complete HIP based framework for secure micro-mobility*. 5th @WAS International Conference on Advances in Mobile Computing and Multimedia, MoMM2007. (pp. 111-122). Jakarta, Indonesia, 3-5 December 2007. ISBN 978-3-85403-230-4

Bokor, L., Nováczki, S., Zeke, T. L., & Jeney, G. (2009). Design and evaluation of host identity protocol (HIP) simulation framework for INET/OMNeT++. In the *Proceedings of the 12-th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems* (MSWIM 2009), Tenerife, Canary Islands, Spain, 26-30 October 2009.

D-ITG. (2009). *Official website*. Retrieved from http://www.grid.unina.it/software/ITG/

Eddy, W. M. (2004, October). At what layer does mobility belong? *IEEE Communications Magazine*, 155–159. doi:10.1109/MCOM.2004.1341274

Fallon, S., Jacob, P., Qiao, Y., Murphy, L., Fallon, E., & Hanley, A. (2008). *SCTP switchover performance issues in WLAN environments*. 5th IEEE Consumer Communications and Networking Conference (CCNC'08), (pp. 564-568).

3GPP TS 23.401 v8.0.0. (2007). *GPRS enhancements for E-UTRAN access (release 8).*

3GPP TS 23.402 v8.0.0. (2007). *Architecture enhancements for non-3GPP accesses (release 8).*

3GPP TS 36.300 v8.3.0. (2007). *Evolved universal terrestrial radio access (E-UTRA) and evolved universal terrestrial radio access network (E-UTRAN).*

Ha, J. S., Kim, S. T., & Koh, S. J. (2005). *Performance comparison of SCTP and TCP over Linux platform. Lecture Notes in Computer Science, 3645/2005* (pp. 396–404). Berlin/Heidelberg, Germany: Springer.

Johnson, D., Perkins, C., & Arkko, J. (2004). *Mobility zupport in IPv6.* IETF RFC 3775, June 2004.

Jungmaier, A., & Rathgeb, E. P. (2006). On SCTP multi-homing performance. *Telecommunication Systems*, *31*(2-3), 141–161. doi:10.1007/s11235-006-6517-7

Kohler, E., Handley, M., & Floyd, S. (2006). *Datagram congestion control protocol*. Internet Engineering Task Force, RFC 4340, March 2006.

Larzon, L. A., Degermark, M., & Pink, S. (2004). *The lightweight user datagram protocol* (UDP-Lite). RFC 3828, Internet Engineering Task Force, July 2004.

Nordmark, E., & Bagnulo, M. (2009). *Shim6: Level 3 multihoming Shim protocol for IPv6*. RFC 5533, Internet Engineering Task Force, June 2009.

Österdahl, H. (2005). *A comparison of TCP and SCTP performance using the HTTP protocol*.

Postel, J. (1980). *User datagram protocol*. RFC 768, Internet Engineering Task Force, August 1980.

Postel, J. (1981). Transmission control protocol. RFC 792, Internet Engineering Task Force, September 1981.

Ratola, M. (2004). *Which layer for mobility? Comparing mobile IPv6, HIP and SCTP*. Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory 2004.

Ravier, T., Brennan, R., & Curran, T. (2001). *Experimental studies of SCTP multi-homing*. First Joint IEI/IEE Symposium on Telecommunications Systems Research, 2001.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., … Schooler, E. (2002). *SIP: Session initiation protocol*. IETF RFC 3261, June 2002.

Schulzrinne, H., Casner, S., Frederick, R., & Jacobson, V. (2003). *RTP: A transport protocol for real-time applications*. RFC 3550, Internet Engineering Task Force, July 2003.

Stewart, R. (2007). *Stream control transmission protocol*. RFC 4960, Internet Engineering Task Force, September 2007.

Wakikawa, R., Devarapalli, V., Ernst, T., & Kagami, K. (2007). *Multiple care-of addresses registration*. (IETF Draft, draft-ietf-monami6-multiplecoa-09.txt), August 2008.

Wakikawa, R., Nishida, Y., & Murai, J. (2006). *The use of SCTP failover mechanism for efficient network handover on mobile IPv6*. 3rd International Symposium on Wireless Communication Systems (ISWCS'06) (pp. 133-137).

ADDITIONAL READING

Stevens, W. R., Fenner, B., & Rudoff, A. M. (2003). *UNIX Network Programming* (*Vol. 1*). Pearson Education.

Stewart, R., & Xie, Q. (2002). *Stream Control Transmission Protocol (SCTP): A Reference Guide*. Addison-Wesley.

KEY TERMS AND DEFINITIONS

SCTP (Stream Control Transmission Protocol): SCTP is a general-purpose transport protocol for the Internet, defined by the IETF and described in RFC 4960. It provides reliable, connection oriented, congestion controlled packet delivery with multihoming and multistreaming capability.

Transport Layer: The fourth layer of the OSI Reference Model protocol stack is the transport layer. It provides necessary functions to enable communication between software application processes on different hosts. Another key function of the transport layer is to provide connection services for the protocols and applications. It may have reliability and flow-control functions as well.

Multihoming: A multihomed host can be reached using more than one IP addresses, usually through more than one network interfaces. This feature allows an endpoint of an association to be mapped to multiple IP addresses.

Multistreaming: Multistreaming makes possible to deliver independent streams within one association. In case of SCTP, each stream has a stream number that is included inside SCTP packets' chunk headers. Multistreaming eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.

LTE (Long Term Evolution): LTE, which often marketed as 4G, is the latest standard in the mobile network technology tree. The LTE specification provides downlink peak rates of at least 100 Mbps, an uplink of at least 50 Mbps.

APPENDIX

Table of abbreviations

AIMD	Additive Increase, Multiplicative Decrease
AP	Application Part
CCID	Congestion Control Identifiers
DCCP	Datagram Congestion Control Protocol
e-NodeB	Evolved NodeB
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
HIP	Host Identity Protocol
HOL	Head of Line
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
LTE	Long Term Evolution
MCoA	Multiple Care-of Addresses
MME	Mobility Management Entity
MSC	Mobile Switching Centre
PMR	Path Maximum Retransmission
QoS	Quality of Service
RTO	Retransmission Timeout
RTP	Real-time Transport Protocol
RTT	Round Trip Time
RTTVAR	Round Trip Time Variation
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
SHIMP6	Site Multihoming by IPv6 Intermediation
SIGTRAN	Signaling Transport
SIP	Session Initiation Protocol
SRTT	Smoothed average of Round Trip Time
SSP	Service Switching Point
STP	Service Transfer Point
TCP	Transmission Control Protocol
TFRC	TCP-Friendly Rate Control
UA	User Adaptation
UDP	User Datagram Protocol