Departament de Teoria del Senyal i Comunicacions
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Evaluation of the SCTP protocol for heterogeneous wireless networks.

Speaker: Łukasz Budzisz

Contact: lukasz@tsc.upc.edu

Supervisors: R. Ferrús, F. Casadevall

Outline

- SCTP – introduction and state of the art
- Motivation: Mobility at transport layer
- Support of mobility in SCTP
- Our research
- Results and discussion

Karlstad University, 10 August 2006

2

First, I will give a brief introduction on the present state of the art of the SCTP protocol for wireless networks. The main open issues in a research will be identified, presenting also a proposed research taxonomy that forms part of the joined work between UPC Barcelona and Karlstad University.

Further on, I will introduce in more details the idea of the handover management at the transport layer constituting the main scope of the thesis, discussing advantages, drawbacks, and its scope of application. Main discussion will focus around the impact of the multihoming feature on congestion control aspects. The review will be illustrated with the already published results.

Regarding the work that needs to be completed within my PhD thesis, I will analyse the following extensions proposed to the SCTP protocol: ADDIP (mobile SCTP), cellular SCTP (including Concurrent Multipath Transfer). Also the work planned during the investigation visit to Karlstad University will be presented.

Stream Control Transmission Protocol (SCTP)

- Defined as a general purpose protocol in:
  - RFCs: 2960, 3309 and 4460 (implementer's guide)
  - Draft: draft-ietf-tsvwg-2960bis-02.txt
- Reliable
- Connection oriented associations
- Multihoming
- Multistreaming
- Congestion control derived from TCP

R. Stewart, "Stream Control Transmission Protocol (SCTP)", IETF draft, June 2006; <draft-ietf-tsvwg-2960bis-02.txt>, work in progress.

Karlstad University, 10 August 2006

3

Stream Control Transmission Protocol (SCTP) is a new IETF's proposal for a general purpose transport protocol. It has been defined in RFC 2960 [1] and later updated in RFC 3309 [2] (header checksum change) and RFC4460 [3] (specification errata and issues).

From March this year, a special draft [4] devoted to further development of the protocol specification was introduced.

SCTP is a reliable transport protocol operating (providing a reliable, full-duplex connection, called association) on top of a connectionless packet network such as IP. It offers the following services to its users:

-- acknowledged, error-free, non-duplicated transfer of user data,

-- data fragmentation to conform to discovered path MTU size,

-- sequenced delivery of user messages within multiple streams (multistreaming), with an option for order-of-arrival delivery of individual user messages,

-- optional bundling of multiple user messages into a single SCTP packet,

-- network-level fault tolerance through supporting of multihoming at either or both ends of an association.

The design of SCTP includes appropriate congestion avoidance behavior and resistance to flooding and masquerade attacks. *(SCTP associations are established in a four-way handshake (instead of a three-way as for TCP) in order to improve protocol security and make it resistant to blind Denial-of-Service (DoS) attacks).*

SCTP was originally designed as a telephony signalling protocol over IP, however its capabilities let extend scope of use as a general use transport protocol, mainly because of its new features: multihoming and multistreaming.

[1] R. Stewart, Q. Xie, et al., "Stream Control Transmission Protocol", IETF RFC 2960 (standard track), October 2000; www.ietf.org/rfc/rfc2960.txt.

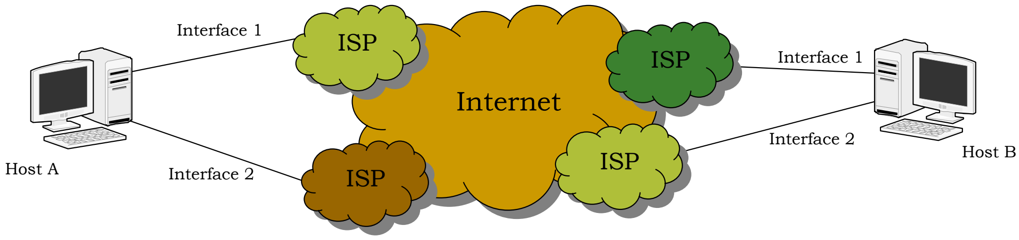
[2] J. Stone, R. Stewart and D. Otis, " Stream Control Transmission Protocol (SCTP) Checksum Change", IETF RFC 3309 (standard track), September 2002; www.ietf.org/rfc/rfc3309.txt.

[3] R. Stewart, I. Arias-Rodriguez, K. Poon, A. Caro, and M. Tuexen, "Stream Control Transmission Protocol (SCTP) Specification Errata and Issues", IETF RFC 4460 (informational), April 2006; www.ietf.org/rfc/rfc4460.txt.

[4] R. Stewart, "Stream Control Transmission Protocol (SCTP)", IETF draft, June 2006; <draft-ietf-tsvwg-2960bis-02.txt>, work in progress.

Multihoming

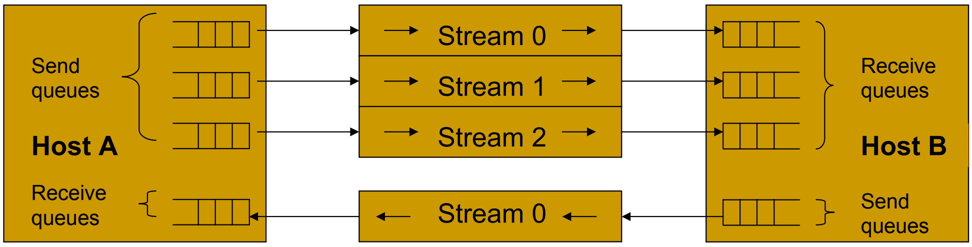
- Multiple IP addresses at each endpoint for single association
- Originally defined only for link redundancy
- Possible scope of use: load balancing



Multihoming support is among the key features of the Stream Control Transmission Protocol (SCTP). Multihoming allows using multiple source-destination IP addresses for a single association between two SCTP endpoints. These IP addresses are exchanged and verified during the initiation of the association, and are considered as different paths between SCTP peers. One of these paths is selected as the primary path, while all the rest are considered as backup or alternative paths. Originally, multihoming was mainly conceived to enhance reliability in environments requiring high availability of the applications, such as signalling transport. Hence its scope of use, defined within the first protocol specification is only for handling single retransmissions, and performing the primary path failover in case of permanent link failure.

Multistreaming

- Stream = unidirectional data flow within an SCTP association
- Within streams: Stream Sequence Number (SSN)
- Between streams no data order preserved
- TCP’s Head-of-Line (HoL) blocking problem limited only to affected stream



Karlstad University, 10 August 2006

5

Multistreaming, allows SCTP establishing associations with multiple streams. Streams are unidirectional data flows within a single association. Number of requested streams is declared on the association setup and valid during the whole association lifetime. Each stream is distinguished with the Stream Identifier field included in each chunk, so that chunks from different streams can be concatenated inside one packet. To preserve order within a stream the Stream Sequence Number is used. Consequently, TCP’s Head-of-Line (HoL) blocking problem is reduced to the affected stream only, not the entire association.

The most important applications of multistreaming that can be mentioned here are:

- priority stream scheduling,

- preferential treatment,

- reducing the latency of streaming multimedia in high-loss environments.

SCTP status

- IETF's Transport Area Working Group (tsvwg)
  - RFCs
  - drafts: 2960-bis, Sockets API Extensions, Mobile SCTP, Transport for the SIP, Security Threats, Telephony Signaling
- Implementations
  - Kernel implementations available on www.sctp.org: Linux (LK-SCTP), FreeBSD (KAME), etc.
  - Socket API for SCTP
- Evaluating SCTP performance
  - Ns-2 SCTP module contributed by University of Delaware
  - QualNet(3.9) SCTP module contributed by University of Delaware

Karlstad University, 10 August 2006

6

SCTP is now subject to a dynamic research, so apart from mentioned RFC and draft defining SCTP, there are various drafts devoted to particular research areas:

-Implementation issues

-Mobility support

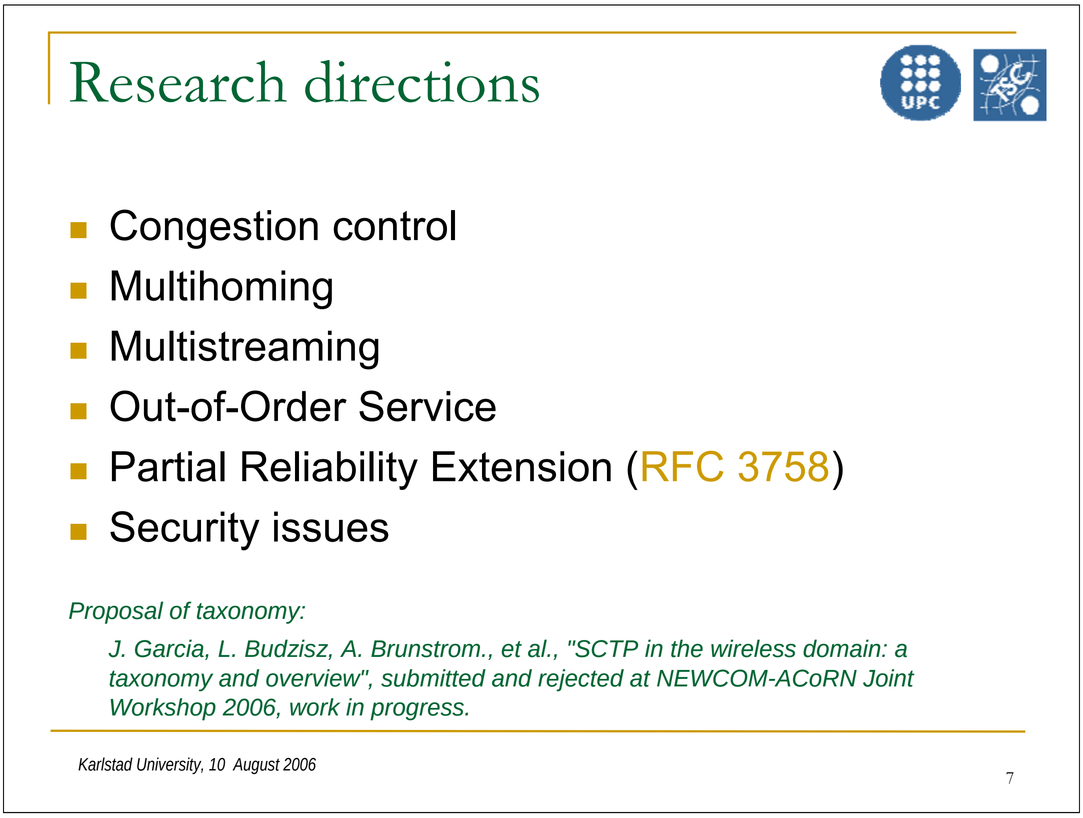
-Security

-Signalling transport

-Application

Various implementations are now available at the kernel or user-space level (more info on: www.sctp.org)

For evaluation of the protocol's performance ns-2 and QualNet SCTP modules were contributed by the University of Delaware research group.



The array (variety) of new features that SCTP offers have attracted researchers from diverse fields. Much SCTP research obviously targets the new functionality and examines it from different viewpoints. The main categories are the following:

- Congestion control
- Multihoming
- Multistreaming
- Out-of-Order Service
- Partial Reliability Extension (RFC 3758)
- Security issues

Many emerging ideas have been brought up and we decided to look for common denominators, which is considerably simplified by the use of a proposed taxonomy. This proposal of a taxonomy provides an overview of selected SCTP research relevant in a wireless context.

This taxonomy for SCTP is constructed using three dimensions:

- Protocol feature examined
- Problem application area
- Study approach

with a number of categories in each dimension.

The aim is to minimize the overlap between the dimensions and the ambiguity into what dimension some aspect of the research relates to. Within each dimension there could, however, be overlap as the research often touches more than a single category in a dimension.

SCTP in wireless domain

Main application areas:

- General transfer
- Transport layer mobility management
- Multi-path transfer
- Multimedia transfer
- Signaling transfer

Karlstad University, 10 August 2006

8

SCTP was originally developed to transport SS7 signaling in IP-based networks. However, since its standardization it has also been considered for a number of other possible uses. This dimensions focus on the application area that the research to be classified relates to. The categories are the following:

General transfer Besides the application areas discussed above, SCTP can also be used as a general purpose transport protocol. The behavior of SCTP in general le transfer type of applications is clearly interesting. Examination of single-homed SCTP provides insights into the general protocol

performance and allows comparison to TCP results. This category is general and thus covers all application areas not explicitly covered in any of the others.

Transport layer mobility management Although originally intended to enhance end-to-end robustness the multihoming functionality of SCTP can also be used as a building block to provide the application layer with transparent handovers. This application area of SCTP has generated considerable interest and is suitable to be discussed in a separate category.

Multi-path transfer Using the multihoming abilities to concurrently transfer data over multiple paths in a load balancing fashion creates both a potential for improved end-to-end performance and a number of complicating issues that need to be addressed. A considerable amount of research has been devoted to this application area which is covered in a separate category.

Multimedia transfer SCTP, and especially together with the PR-SCTP extension that provides partial reliability, can be used to transfer multimedia data. The multistreaming capabilities of SCTP maps well to multimedia traffic having multiple media streams. This application area has its own set

of challenges and is therefore handled in a separate category.

Signaling transfer Since SCTP was originally designed for transporting SS7 signaling the performance in this application domain is important. SCTP can also be used to transfer other kinds of signaling traffic such as Session Initiation Protocol (SIP). Signaling transport is one of the major applications for SCTP and thus has its own category.

Further in this presentation we will focus at the **transport layer mobility management** as the main scope of my thesis. First of all motivation behind that should be given.

Motivation – Mobility Management Support

Category	**MobileIP**	**SIP**
Layer	Network	Application
Location Management Support	yes	yes
Handover Management Support	FMIP needed	Not supported
Route optimization	Binding update needed	Not provided
Network Support	Required	Not required
Special Agents	Home Agent, Foreign Agent	SIP Servers

M. Eddy, "At what layer does the mobility belong?" IEEE Communications Magazine, vol. 42, no. 10, pp. 155-159, October 2004.

One of most important aspects in the introduction of the IP into mobile communication networks is the mobility management. Mobility management includes two fundamental operations: location and handover management. According to [1], handover management deals with all the necessary challenges to change the attachment point of a Mobile Host (MH), while maintaining the communication with the correspondent node (CN), such as, notifying the CN about the change, migrating the connection from the old access point (AP) to the new one, change scheme and policy, to mention the most significant ones. Location management focuses on keeping track of the current IP address of an MH, and providing the valid address to any entity that needs to communicate with the MH, while being transparent to the peers.

Earlier works on the mobility management problem in the heterogeneous networks discussed solutions in different layers of the protocol stack. For example, SIP, MSOCKS, MobileIP, Mobile Ethernet, are application, transport, network and data-link layer schemes, respectively. Here in the table a comparison of different proposals is given.

However [2] concludes that the transport layer is the most promising solution.

[1] M. Riegel and M. Tuexen, "Mobile SCTP", IETF draft, March 2006; <draft-riegel-tuexen-mobile-sctp-06.txt>, work in progress

[2] M. Eddy, "At what layer does the mobility belong?" IEEE Communications Magazine, vol. 42, no. 10, pp. 155-159, October 2004.

Mobility at transport layer

- Handled by both endpoints of the network
- Transparent to the application layer
- Change of the IP address possible, while the end-to-end connection is alive

M. Riegel and M. Tuexen, "Mobile SCTP", IETF draft, March 2006; <draft-riegel-tuexen-mobile-sctp-06.txt>, work in progress

Karlstad University, 10 August 2006 10

According to the [1] we define transport layer mobility as a mobility handled by both endpoints of the connection transparently for the application layer protocols, except of those using IP addresses in their messages. A mobility enabled transport protocol supports the change of the IP address of the underlying network layer while keeping the end-to-end connection alive.

[1] M. Riegel and M. Tuexen, "Mobile SCTP", IETF draft, March 2006; <draft-riegel-tuexen-mobile-sctp-06.txt>, work in progress.

Mobility at transport layer [2]

- **Advantages:**
  - Similar to the nature of Internet: network layer provides connectivity only, the entire functionality is located at both endpoints
  - No special agents needed
- **Drawbacks:**
  - Location management is not supported
  - Several transport protocols used in IP networks

M. Atiquzzaman and A. Reaz, "Survey and Classification of Transport Layer Mobility Management Schemes," Proc. the 16th IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2005), pp., September 2005.

Karlstad University, 10 August 2006

11

As a consequence these are the following advantages and drawbacks of proposed solution:

A full survey of transport layer mobility solutions is available in the article:

[1] M. Atiquzzaman and A. Reaz, "Survey and Classification of Transport Layer Mobility Management Schemes," Proc. the 16th IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2005), pp., September 2005.

Support of mobility in SCTP

- Standard SCTP defined in:

- RFCs: 2960, 3309 and 4460 (implementer's guide)
- Draft: draft-ietf-tsvwg-2960bis-02.txt

- Mobile SCTP (mSCTP), the ADDIP extension

- Cellular SCTP (cSCTP)

R. Stewart, "Stream Control Transmission Protocol (SCTP)", IETF draft, June 2006; <draft-ietf-tsvwg-2960bis-02.txt>, work in progress.

Karlstad University, 10 August 2006

12

Within the SCTP area nowadays, we have identified the following possibilities to provide transport layer mobility:

•Standard SCTP

•Mobile SCTP

•Cellular SCTP

Each of the proposals will be discussed here in more details

Mobile SCTP (mSCTP)

- ADDIP extension – dynamic address reconfiguration
  - draft-ietf-tsvwg-addip-sctp-14.txt defines new chunk types: ASCONF(0xC1), ASCONF-ACK(0x80)
  - Adding new or deleting unnecessary IP addresses from the existing SCTP association
  - Changing the primary IP address for the SCTP association

R. Stewart, M. Ramalho, Q. Xie, M. Tuexen and P. Conrad, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", IETF draft, March 2006; <draft-ietf-tsvwg-addip-sctp-14.txt>, work in progress.

Karlstad University, 10 August 2006 13

In order to make the SCTP protocol a mobility enabled transport protocol an ADDIP extension was defined in [1]. The ADDIP extension enables the SCTP to dynamically add or delete IP addresses and request the change of the primary IP address during an active SCTP association, by means of two new chunks: Address Configuration Change Chunk (ASCONF, chunk type: 0xC1) and Address Configuration Acknowledgement (ASCONF-ACK, chunk type: 0x80) and six new parameters: Add IP Address, Delete IP Address, Set Primary Address, Error Cause Indication, Success Indication, Adaptation Layer Indication.

According to the [2] the only requirements for the mSCTP are as follows: mobile host (MH) MUST support an ADDIP extension whereas the CN in addition to this MUST also use multiple IP addresses.

[1] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen and P. Conrad, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", IETF draft, March 2006; <draft-ietf-tsvwg-addip-sctp-14.txt>, work in progress.

[2] R. Stewart, I. Arias-Rodriguez, K. Poon, A. Caro, and M. Tuexen, "Stream Control Transmission Protocol (SCTP) Specification Errata and Issues", IETF RFC 4460 (informational), April 2006; www.ietf.org/rfc/rfc4460.txt.

Mobile SCTP (mSCTP) [2]

- Challenging issue:
  - Add/delete/change primary IP criteria:
    using lower-layer information, using upper-layer information, avoiding oscillations
- mSCTP limitations:
  - Simultaneous handover at both endpoints is not supported
  - Slow start may occur, when oscillating between neighbouring APs

Karlstad University, 10 August 2006

14

- Criteria to add, delete IP, change primary.

Obtaining new IP address may rely on the support of wireless signalling control at the physical layer.

However, as stated in [1], the most challenging issue of the mSCTP is to specify the rules for changing the primary IP. Some triggering rules that may be considered are:

As soon as a new IP address is detected: good solution for fast moving MH, especially in terms of the handover latency. Less desired in the scenarios with so called ping-pong effect (when MH oscillates between neighbouring APs).

By using indication from the lower layer: physical layer compares the strength of the received signal from both addresses and decides when the SCTP sends the ASCONF message. This solution seems to be most preferred choice according to the [2] as it permits avoiding ping-pong effect.

By using indication from the upper layer: this solution can be especially preferable for intersystem or vertical handovers (i.e. WLAN and UMTS) considering the trade-off: between the coverage, available bandwidth and cost of the connection for different systems.

Also deleting IP address should be performed according to some rules. The most reasonable solution seems to be the signal strength measurement received from the physical layer

- What is the benefit to add an extra address, if available, and its cost, if one.

Benefit of the mSCTP solution is that only requirement that both nodes should support mSCTP implementations without any changes to the intermediate nodes

Still an open issue.

- Drawbacks of the mSCTP:

The mSCTP does not handle simultaneous handover of both SCTP endpoints. If both ends perform a handover at the same time, association will be lost. However mSCTP can handle sequentially occurring handovers at both ends.

Triggering conditions to force the primary path change may provoke oscillations between neighbouring APs, so it is fundamental to provide good rules in order to avoid signalling traffic overhead.

It is also important to mention that the mSCTP is targeted for mobile sessions originated from MH towards the CN as the mSCTP does not support location management. Therefore to support location management as for sessions originating form the CN along with the mSCTP an additional protocol must be used such as MobileIP or SIP or RSerPool as stated in [1].

Additionally there are two drafts [2] and [3] commenting additional aspects of mSCTP extension

[1] M. Riegel and M. Tuexen, "Mobile SCTP", IETF draft, March 2006; <draft-riegel-tuexen-mobile-sctp-06.txt>, work in progress.

[2] S. J. Koh and Q. Xie, "Mobile SCTP (mSCTP) for Internet Mobility", IETF draft, October 2005; <draft-sjkoh-msctp-01.txt>, work in progress.

[3] S. Maruyama and M. Kozuka, “Stream Control Transmission Protocol(SCTP) Cumulative ASCONF chunk transmission extension", IETF draft, October 2005; <draft-marushin-sctp-asconfext-01.txt>, work in progress.

Cellular SCTP (cSCTP)

- Further extensions to the mSCTP:

- Additional handover procedure
- New state variable indicating handoff mode
- During handover phase packets are duplicated at the CN: both addresses are considered as primary addresses, cwnd is reduced to the half of the old value

I. Aydin, W. Seok, and C.-C. Shen, "Cellular SCTP: a transport-layer approach to Internet mobility," Proc. the 12th International Conference on Computer Communications and Networks (ICCCN 2003), pp. 285-290, October 2003.

Karlstad University, 10 August 2006 15

The cSCTP introduces a new state variable called handoff_mode (the ASCONF and ASCONF-ACK chunks contain modified flag field, with on bit flag H indicating handoff_mode) to mark the start of the handover procedure. After cSCTP obtains information about a new IP address an MH sets its handoff_mode value to true, sends an ASCONF message to the CN to inform the CN that handover has started, and adds the new IP address. The CN upon receiving the ASCONF chunks follows the changes: modifies handoff_mode variable, adds the new address (and responses with ASCONF-ACK chunk I suppose, that was not mentioned in the article). However during the handover both addresses are considered as primary addresses to the MH. Congestion window (cwnd) size for each path is set to the half of the old primary address value. Therefore the CN duplicates packets and sends them to the both addresses.

Removing an inactive IP address (determined by a certain policy: no received data from CN on that path address or no routing advertisements from the old AR) looks similar: first the MN turns off the handoff_mode, removes unnecessary IP address and sends an ASCONF chunk with Delete-IP parameter towards the CN. The CN follows these steps and responses with ASCONF-ACK chunk using from that moment only one, new primary address

Cellular SCTP (cSCTP) [2]

- Possible weak points:

- Duplications at the MH
- Initial cwnd size for the new path
- Different path behaviour not considered

Karlstad University, 10 August 2006

16

CN duplicates packets and sends them to the both addresses:

That could provoke duplications at the MH, however reduces the risk (existing with the mSCTP) of losing packets sent to the old primary path, in case it becomes unreachable before the change of the primary address to the newly added one.

Research summary

1. SCTP in a dynamically changing channels

   L. Budzisz, R. Ferrús, F. Casadevall, "On the performance of multihoming SCTP in dynamically changing radio channels ," Proc. the 15th Mobile and Wireless Summit, June 2006.

2. Link-layer retransmissions influence on the SCTP performance

   L. Budzisz, R. Ferrús, F. Casadevall, "SCTP multihoming performance in dynamically changing channels with the influence of link-layer retransmissions ," will appear in Proc. the 64th IEEE Vehicular Technology Conference (VTC 2006Fall), September 2006.

3. Initial study on mSCTP triggering conditions

   L. Budzisz, R. Ferrús, F. Casadevall, " Study on Transport Layer Handover using SCTP," Proc. the 9th Wireless Personal Multimedia Communications (WPMC 2005), September 2005.

Karlstad University, 10 August 2006

17

First I would like to present a summary of the work performed so far.

The milestones are marked with the following publications:

1.) L. Budzisz, R. Ferrús, F. Casadevall, "On the performance of multihoming SCTP in dynamically changing radio channels ," Proc. the 15th Mobile and Wireless Summit, June 2006.

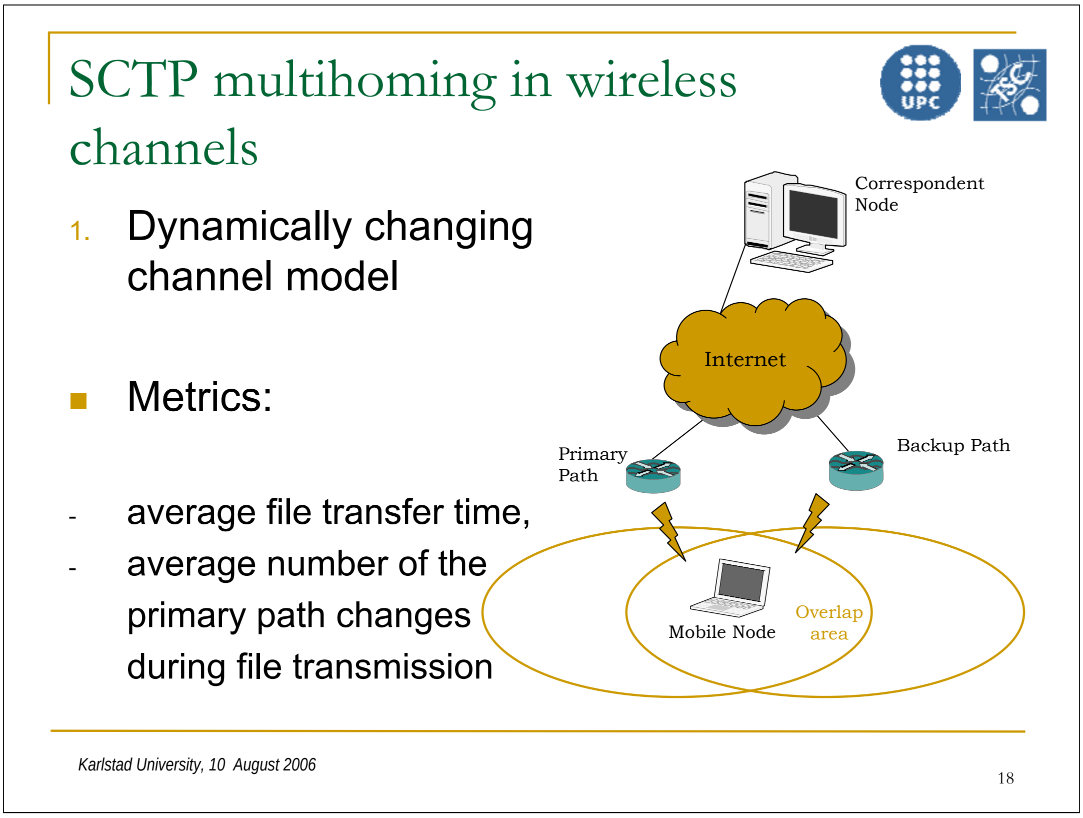
Standard SCTP's design was not targeted to cope with the variable nature of wireless channels and most performance analysis published so far have been addressed to static channel conditions. Consequently this paper will focus on the analysis of the standard SCTP failover performance in multihoming scenarios that change dynamically and could serve as a reference point for further investigation of handling mobility management problem at the transport layer. Obtained results make evident the trade-off between stable and fast performance under specific channel conditions and for different Path Maximum Retransmissions (PMR) settings.

2.) L. Budzisz, R. Ferrús, F. Casadevall, "SCTP multihoming performance in dynamically changing channels with the influence of link-layer retransmissions ," will appear in Proc. the 64th IEEE Vehicular Technology Conference (VTC 2006Fall), September 2006.

The performance of SCTP protocol is assessed, under different radio channel variation patterns and different degrees of link level reliability. Obtained results are claimed to be a reference point for further investigation related to new proposals for handover schemes handled at the transport layer.

3.) L. Budzisz, R. Ferrús, F. Casadevall, " Study on Transport Layer Handover using SCTP," Proc. the 9th Wireless Personal Multimedia Communications (WPMC 2005), September 2005.

In this paper we perform initial study of SCTP performance in order to evaluate the idea of soft handover in the transport layer. We discuss two different aspects: the influence of the point between two adjacent Access Points to trigger the handover, and a set of triggering rules based on radio signal strength. From the experiments on triggering rules it was shown that the best trade-off between average throughput and signalling overhead is achieved for a slow add-IP and fast change-IP.



First, I present results for an evaluation of the SCTP protocol performance in a wireless channel that change dynamically, when sending a 16 MB file via FTP.

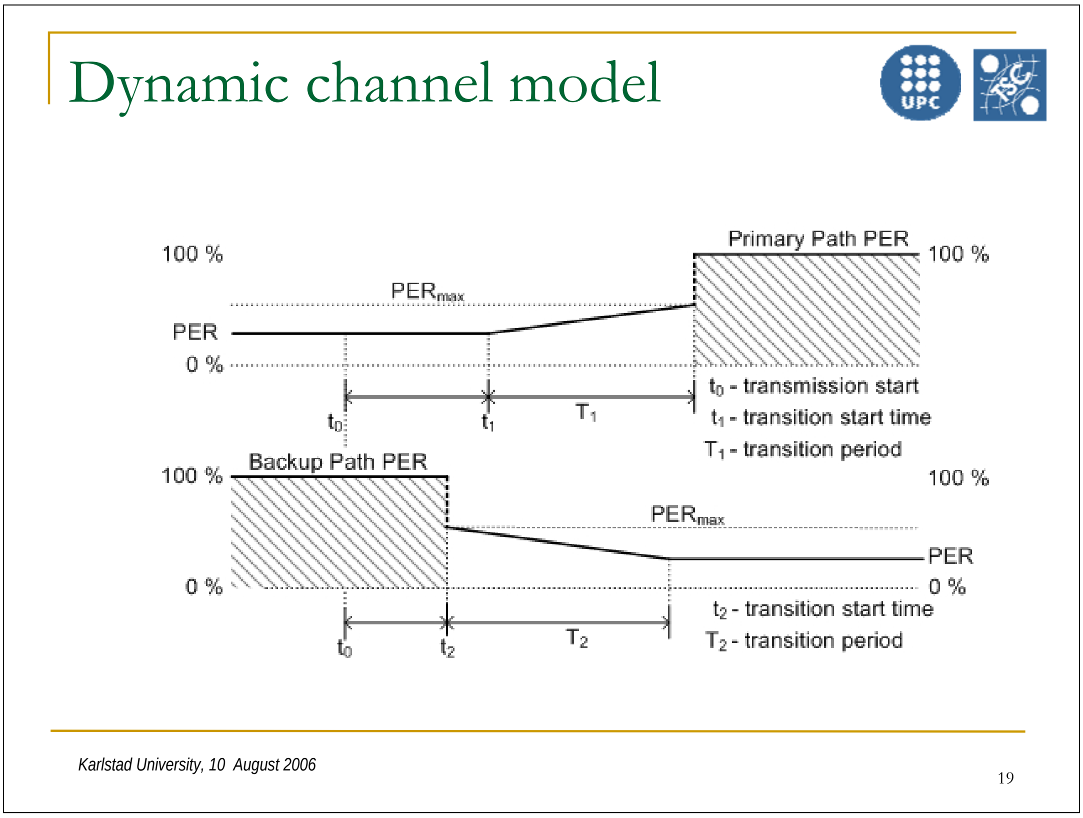
To measure the protocols' performance we use two types of metrics:

- average file transfer time,
- average number of the primary path changes during file transmission

The proposed simulation topology, presented at the figure, shows a symmetrical scenario, both paths (primary and backup) from the sender to the receiver consist of the wired and wireless parts, with the wired parts' bandwidth of 100 Mbps and 5ms delay (100BaseT), and the wireless parts with 11 Mbps bandwidth and 15 ms delay (WLAN) respectively, so the bandwidth delay product (BDP) is adjusted to the typical 3G networks values. For the considered scenario we introduce an ideal and real channel models described in details further.

We introduce dynamically changing channel model in order to expose protocol's performance

For the standard SCTP we also try to estimate the failover time, measured from the moment when the failure occurs till the time the new path is selected as the primary path (the sender fails over to a new path).



We introduce the linear error model for both paths, and the resulting channel model is shown on the figure. This model stands for two radio channels that can be acquired by the mobile user at different points of time with different link quality. As before, the upper limit of the PER values is set to PERmax, and beyond this limit the channel becomes inaccessible. The primary link starts to deteriorate after t1 time from transmission start, and after T1 from that point becomes unavailable, whereas the backup link becomes accessible after t2 from transmission start, with PERmax as a starting value and improves to the PER level after T2 transition time.

Performance in this channel model will be compared to the performance in a static channel (as widely used in a literature)

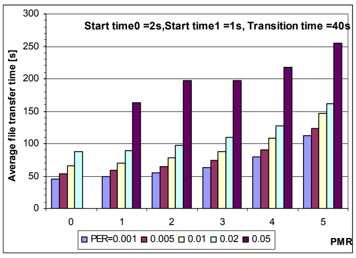
Scenario parameters

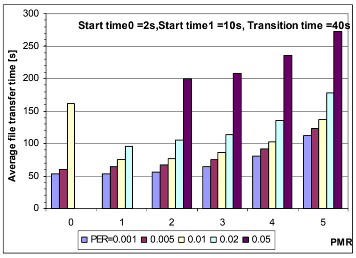
Parameter	Value/range
Transition start time (t_1 and t_2)	0-10 s (8 values)
Transition period (T_1 and T_2)	0-40 s (5 values)
Packet Error Rate at the link-layer (PER)	0.1-10% (6 values)
PER threshold (PER_{max})	20%
Buffer size	50 packets
Retransmission handling	FastRtx SamePath TimeOut Alt Path
Path Maximum Retransmissions (PMR)	0-5 (6 values)
Association Maximum Retransmissions	10
Heartbeat Interval	30 s
MTU size	1500 Bytes
Payload size	1468 Bytes
Downloaded file size	16 MB
Maximum allowed transmission time	900 s

Channel without errors: transmission time= 13,4s

Dynamic channel model results

- PMR value is the most significant factor
- Quite stable for low PER rates (1% or less), unstable performance for bigger PER rates
- For bigger PER, only PMR 3 or bigger guarantees stable transmission (tradeoff)





Karlstad University, 10 August 2006

21

We perform the analysis for the proposed dynamic channel model.

We can observe that **the PMR value has the biggest impact** (much bigger when compared to the impact of rest of parameters). However, this effect is **further strengthened by the PER value**, as it can be observed for the transition time=20s. For the values of the PER lower than 10% , the bigger the PER is, the longer is the average file transfer time. Beyond this point, the low quality of the link provokes earlier change of the primary link and as the backup path has no errors the transmission is completed faster.

The most important tendency that can be observed in the graphics presented in the figure is that for low PER rates (i.e., 1% or lower) the standard SCTP failover mechanism presents quite stable, even if the standard PMR value is decreased to 0 in order to achieve faster file transmission. Further on, as the PER value increases to 2% stable transmission is achieved with PMR set at least to 1 (any of 10 probes for the PMR=0 does not succeed), whereas for the biggest possible PER rate (10%) the lowest PMR that allowed successful file transmission in less than 900 seconds was 3. The trade-off is paid with the time of transmission that is around 700 seconds, and not varying much within three biggest values of PMR.

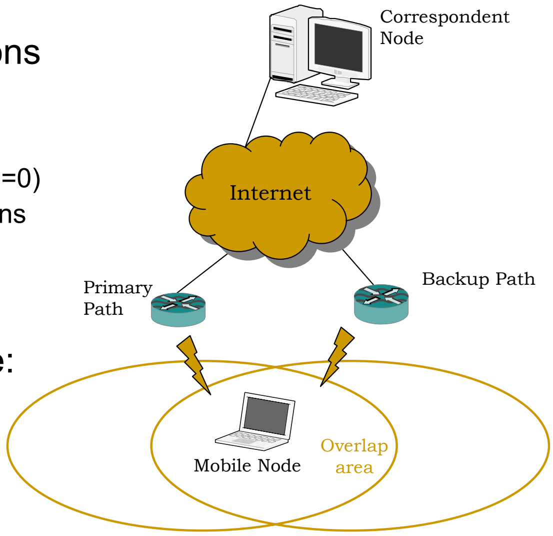
When compared to the reference scenario, proposed channel model excludes lower values of PMR, as unstable for the bigger PER values, but as a result also huge number of primary changes is reduced, as can be seen at the figure. Of course, the larger the transmission time is, the closer to the reference scenario, and number of changes increases, but still for the biggest transition time investigated (40s), the average number of changes was lower than 25 (when the primary link failure (T1) starts at 1s); here in the figure, the average result for the start time T1=2s, and the lowest value obtained was about 13 for the start time T1=8s). If more changes occur, as for PER values bigger than 1% and low PMR

SCTP multihoming in wireless channels [2]

2. Link layer retransmissions influence:

- No retransmissions available (δ=0)
- Several link layer retransmissions (δ>0)
- Infinite retransmissions (δ= ∞)

■ Same metrics as before:
- average file transfer time,
- average number of the primary path changes during file transmission



Karlstad University, 10 August 2006

22

Now using the same metrics as before we introduce the link layer retransmissions.

We analyse three diferent cases:

-No retransmissions available (δ=0)

-Several link layer retransmissions (δ>0)

-Infinite retransmissions (δ= ∞)

we considered FEC-ARQ mechanism as a basic form of protection from the non-congestion losses in the radio channel.

To measure the protocols' performance we use two types of metrics:

- average file transfer time,
- average number of the primary path changes during file transmission

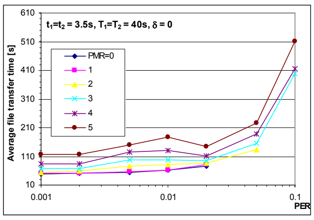
The proposed simulation topology, presented at the figure, shows a symmetrical scenario, both paths (primary and backup) from the sender to the receiver consist of the wired and wireless parts, with the wired parts' bandwidth of 100 Mbps and 5ms delay (100BaseT), and the wireless parts with 11 Mbps bandwidth and 15 ms delay (WLAN) respectively, so the bandwidth delay product (BDP) is adjusted to the typical 3G networks values. For the considered scenario we introduce an ideal and real channel models described in details in further paragraphs.

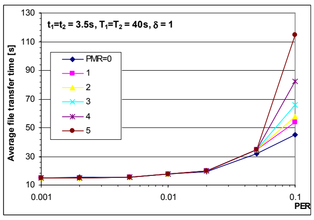
Scenario parameters

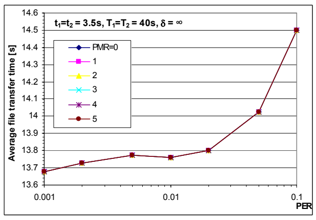
Parameter	Value/range
Transition start time (t_1 and t_2)	0,5-9,5 s (4 values)
Transition period (T_1 and T_2)	0-40 s (5 values)
Packet Error Rate at the link-layer (PER)	0.1-10% (6 values)
PER threshold (PER_{max})	20%
ARQ persistency	0-∞ (9 values)
Buffer size	50 packets
Retransmission handling	FastRtx SamePath TimeOut Alt Path
Path Maximum Retransmissions (PMR)	0-5 (6 values)
Association Maximum Retransmissions	10
Heartbeat Interval	30 s
MTU size	1500 Bytes
Payload size	1468 Bytes
Downloaded file size	16 MB
Maximum allowed transmission time	900 s

We introduced different values of ARQ

Link layer retransmissions influence





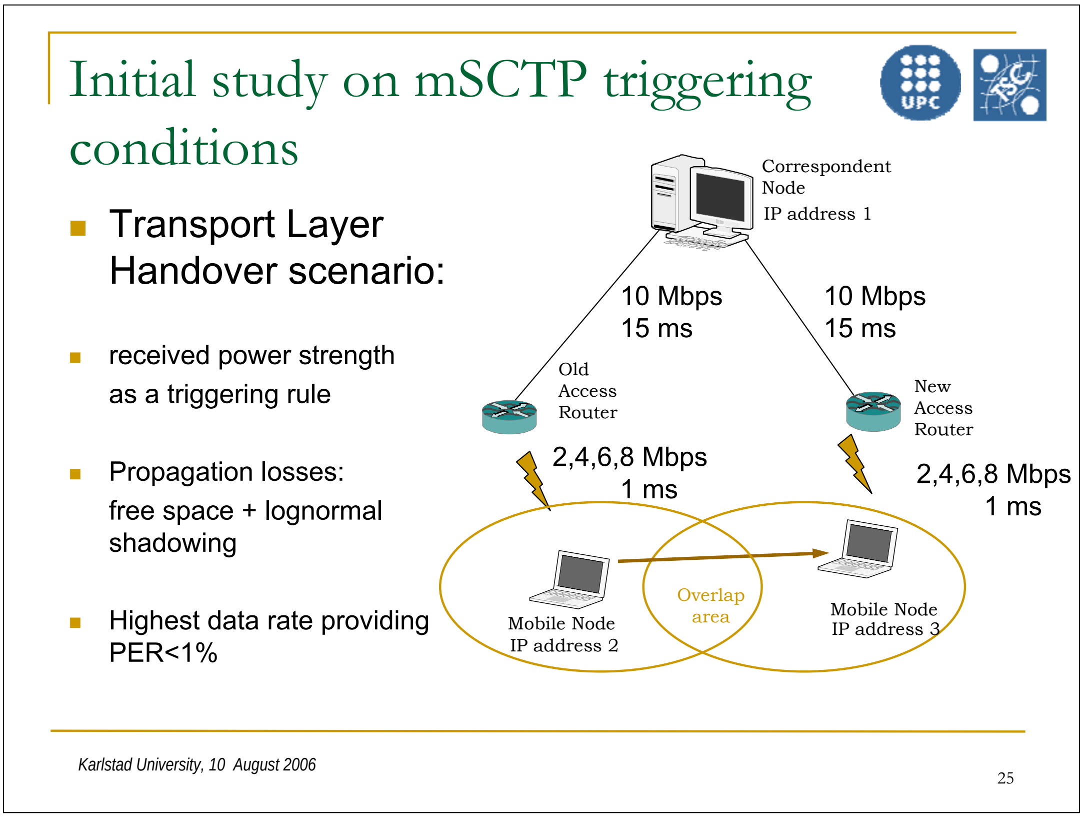


- For low error rates (PER<2%) fairly good performance even in non-shielded channels
- Any shielding at the link layer improves significantly protocols' performance, so PMR value may be decreased even in channels with high PER rates

•Following the TCP's experience with noisy radio channels, channel not protected at the link layer leads to weak SCTP performance either, forcing transmission times around 500s for the highest 10% PER rate (about 40 times bigger than in channel without errors - 13.4s), and about 120s for the lowest PER rate investigated 0.1% (9 times bigger than errorless transmission, respectively). Introducing any shielding at the link layer improves significantly the overall protocol's performance, leading finally to a very stable and fast performance, when many retransmissions are allowed.

•Shielding on the link layer is also visible in terms of number of the primary path changes. In a non-shielded wireless channel, when the whole impact of non-congestion losses goes directly to the transport layer, Path Maximum Retransmissions (PMR) parameter plays the role of the stabilising factor. For low error rates (i.e., PER below 2%) it is possible to obtain fairly high throughput rates decreasing the PMR value from the default 5 down to 1. PMR set to 0 even for low PER rates provokes so called "ping-pong" effect and the gain in throughput is not that significant, as if compared to the PMR set to 1. Further on, as the PER value increases beyond 2%, only higher PMR values guarantee stable file transmission, however as it was mentioned above the trade-off results in fairly long transmission time, because of exponential back-off mechanism that triggers handover. Meanwhile, with low PMR values (i.e., 0 or 1) file transfer cannot be completed within 900 seconds time in a non-shielded channel. For partially shielded channel (δ = 1), also the lower PMR values can result in successful file transmission, even if the PER achieves rates as high as 10%. That practically guarantees reliable and fast file transmission. As for channel without losses (δ = ∞), all the impact of varying radio channel is handled on the link layer, and therefore preventing from forcing any failover at the transport layer. Such policy however, could result in spurious retransmissions or even timeouts for very noisy channels. Nevertheless, in the analysed case, the highest PER rate taken into account 10% (that corresponds to PER rates varying between 10 and 20% in the proposed channel model) was not big enough to provoke that.

•In this paper we have evaluated the standard SCTP in a simple dynamically changing multihoming scenario in order to expose protocol's performance under progressively deteriorating channel conditions that finally lead to the non-availability of the primary interface and force the failover. In particular, we considered FEC-ARQ mechanism as a basic form of protection from the non-congestion losses in the radio channel. In this sense, for not shielded channels with low error rates (i.e., PER below 2%), it is possible to obtain fairly high throughput rates decreasing the PMR parameter from the default value of five to one or zero. The same low PMR values, as the error rate increases beyond 2%, result in unending oscillations between two paths, decreasing therefore the protocol's performance. Hence, only higher PMR values guarantee stable file transmission, resulting in fairly long transmission times because of exponential back-off mechanism used in the failover process. On the other hand, for partially or fully shielded channels, improvements introduced by the FEC-ARQ mechanism in the multihoming scenario allow preserving lower PMR values, even if the PER achieves rates as high as 10%.



In this scenario, the mobile user starts moving from one access point to the other, while maintaining an active SCTP association with the correspondent node. The decision of changing the network attachment point, as well as the execution of this process may have an important impact on the protocol performance and such analysis will form the scope of this paper.

The simplest simulation model comprise of the symmetrical links when changing the attachment point from old AP to the new AP. Propagation path losses are accounted by a free space model plus a lognormal shadowing model with a standard deviation 5dB, and correlation distance of 10m. Under such constructed scenario, different decision functions, considering the relation of received signal strength from both APs, were evaluated

Radio channel transmissions are carried out at 8, 6, 4 and 2 Mbits/s data rates. A link adaptation algorithm assures the highest data rate among those, while providing a packet loss ratio below 1%. No channel coding is used so packet loss ratio is directly obtained from the radio channel bit error ratio (that depends on the M-QAM modulation, the observed signal to noise ratio) and the number of bits of a packet.

Scenario parameters

Parameter	*Value*
Transmitted power, each AP	20 dBm
Noise level	-174 dBm/Hz
Wired line transmission delay	15 ms
Bandwidth of the wired networks	10 Mb/s
Distance between APs	162 m
Mobile node speed	2 m/s
Number of possible states for each M-QAM modulation	4, 16, 64, 256
Symbol transmission speed	1 Msymbol/s
Packet loss threshold	1%
SCTP data chunk size	1468 Bytes

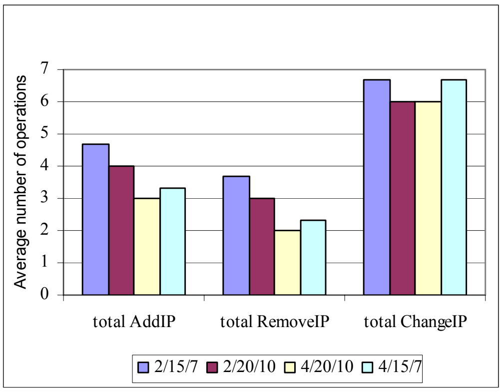
Metrics:

Throughput rate

Number of changes

Evaluation of SCTP performance

- Different handover policies:
- Fast add-IP, Fast Change IP
- Fast add-IP, Slow Change IP
- Slow add-IP, Fast Change IP
- Slow add-IP, Slow Change IP



Average number of operations in the overlap area for different handover policies.

Very important feature in study of transport layer handover are triggering rules. We use standard relative signal strength criterion to determine when introduce a new IP address, change the primary IP or remove unnecessary IP address. Measurements are done each 20ms, and the following triggering levels are considered:

•Fast add-IP, if for 2 consecutive measures signal of a new AP is stronger than current, then a valid IP address for the new AP is added to the association.

•Slow add-IP, the same as before, but now within 4 consecutive probes meeting such criterion.

•Fast change-IP, changing primary IP address after 7 consecutive probes

•Slow change-IP, primary IP change with 10 probes threshold.

We also set thresholds levels for the Remove-IP address, which are 15 and 20 probes for fast and slow Remove-IP respectively. Figures 6 and 7 present the performance comparisons for each of mentioned triggering rules (thresholds are shown in the following order: Add-IP/Remove-IP/Change-IP). Each simulation was run 3 times to achieve the average performance.

Further investigation directions

- Further evalution of mSCTP proposal:
  - Evaluation of the complete mSCTP scenario in a dynamic channel
  - Looking for best triggering criteria
- Evaluation and extension of the cSCTP performance:
  - Comparison with mSCTP

Further investigation directions [2]

- Employing different Concurrent Multipath Transfer (CMT) policies to the cSCTP

- Performance of the CMT under varying bandwidth proportions. Possibly extension to the study:
  J. Iyengar, P. Amer, and R. Stewart, "Concurrent multipath transfer using transport layer multihoming-Performance under varying bandwidth proportions," Proc. IEEE Military Communications Conference (MILCOM 2004), October 2004.

- Performance of the CMT for different retransmission policies:
  J. Iyengar, P. Amer, and R. Stewart, "Retransmission policies for concurrent multipath transfer using SCTP multihoming," Proc. the 12th IEEE International Conference on Networks (ICON 2004), vol. 2, pp. 713-719, November 2004.

- *Bandwidth-aware source scheduling:*
  C. Casetti, G. Galante, and R. Greco, "Load balancing over multipaths using bandwidth-aware source scheduling," Proc. the 7th International Symposium on Wireless Personal Multimedia Communications (WPMC 2004) , September 2004.

1. for different bandwidth and link delay values

Summary

- SCTP – state of the art in wireless research
- Mobility management at transport layer
- 3 proposals to support of mobility in SCTP
- Our research
- Research visit to Karlstad University

Research visit to Karlstad

Task proposed:

1. Further extension to the taxonomy proposal:
   - new submission format: proposal for the joined journal publication
2. Transport layer handover scenarios:
   - mSCTP scenarios
   - Study on CMT cases
3. Analytical estimation of failover time - proposal
   - Explaining the T3-rtx management rules
   - New factor(s) introduced to the timeout estimation

Karlstad University, 10 August 2006

31

1. proposal for the joined journal publication, description of the protocol + open points identification + proposed taxonomy

2. mSCTP and CMT scenarios

3. T3-rtx timer functionality

Departament de Teoria del Senyal i Comunicacions
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Questions?