# A New Path Failure Detection Method for Multi-homed Transport Layer Protocol

Sinda Boussen, Nabil Tabbane and Sami Tabbane
Research Unit MEDIATRON (SUP'COM)
University of 7th November at Carthage
Tunisia
{sinda.boussen, nabil.tabbane, sami.tabbane}
@supcom.rnu.tn

Francine Krief
CNRS-LaBRI Laboratory
University of Bordeaux, IPB
France
krief@labri.fr

***Abstract*—Through its support for multi-homing, the Stream Control Transmission Protocol (SCTP) is a suitable solution to implement and manage user's mobility by abstracting multiple physical paths into a single end-to-end association. In order to detect the primary path failure, SCTP uses a strategy defined in the RFC2960 and mainly based on a retransmission time out (RTO). When a number of retransmission failures occur on the primary path, switchover procedure is initiated which means that a new primary path will be selected among the available secondary paths. In this paper, we investigate the current switchover mechanism implemented in SCTP and detail some of its deficiencies which affect the use of SCTP in a WLAN environment. Then we propose a new path failure detection strategy designed to perform path management more efficiently in wireless environment, by preempting path failure and avoiding service interruption. Finally, we outline the testing of this new strategy in the context of a WLAN environment and the results are compared to those obtained when using the standard SCTP strategy.**

***Keywords- SCTP; multi-homing; RTO; path failure detection; WLAN.***

## I. INTRODUCTION

The Stream Control Transmission Protocol (SCTP) [7] was initially developed by the Internet Engineering Task Force (IETF) to transport signaling messages over IP networks. Compared to other transport protocols like TCP and UDP, SCTP provides additional features which are multi-homing and multi-streaming. These features make it suitable for the transport of many services which use the classical transport protocols. Currently, many applications are migrating to SCTP in order to take advantage of the new features offered by this protocol.

In SCTP terminology, an association is a connection between two endpoints which is identified by a source port and a destination port. An SCTP message contains the common SCTP header and various control or data chunks. By supporting multi-homing, SCTP is able to implement an end-to-end session transparently over multiple physical paths where the endpoint of each path is identified by an IP address. At the set up of an SCTP association, each endpoint provides a list of transport addresses composed of one or more IP addresses and a SCTP port. One of the IP addresses is used for the establishment of the primary path that is used for data chunks transmission. The other paths, called secondary paths, are used for data retransmission to increase reliability.

Moreover, through its support for multi-homing, SCTP represents a suitable solution to implement and manage user's mobility. Indeed, the primary path used for data transmission can be modified while maintaining the session. This property enables guaranteeing service continuity that is very important in some applications that rely on real time communications, such as Voice over IP (VoIP) and video streaming applications.

For that purpose, SCTP needs a path management mechanism to detect primary path failure and initiate the path switchover when necessary. The standard strategy to detect path failure, which is defined in the RFC2960, is based mainly on a retransmission Timeout (RTO). In fact, data transmission failure occurs when the timer RTO is expired without that the data sent are acquitted. Then, if the number of retransmission attempt reaches a predefined threshold called PMR, SCTP is going to activate the path switchover procedure which means that current path will be set to INACTIVE state and a new primary path will be selected.

The motivation behind this paper is a need to have a more accurate estimation of the failover (path failure) time in SCTP by interpreting the network quality degradation as an indicator of imminent primary path failure and implementing an immediate path switchover.

This paper is organized as follows. Section II details related work in the area. Section III describes in detail SCTP path management functionality. In Section IV, we propose an enhancement of the SCTP path failure detection strategy in order to preempt and avoid path failures in wireless environment. Then, Section V describes the simulated study undertaken and presents results. Finally, Section VI concludes the paper and points out future work.

## II. RELATED WORK

In the current SCTP implementation, the path switchover strategy is reactive which means that switchover will only

 ISBN:978-1-61208-002-4 

occur once the primary path has failed and the primary destination address is marked as INACTIVE. A number of studies have been undertaken, which investigate the performance of SCTP switchover in wireless networks.

In [1], authors show that the current SCTP mechanism for calculating RTO value is inappropriate in WLAN environments, by identifying significant deficiencies which affect the use of SCTP in a WLAN environment. These deficiencies result from the mechanism by which SCTP determines when a path switchover should be initiated. Experimental results indicate that SCTP allows more time to switchover as network conditions degrade.

In order to reduce the switchover performance deficiency experienced in WLAN environments, authors in [2] investigate the performance implications of changes to the SCTP RTO mechanism, particularly alterations to the parameters α, the smoothing factor, and β, the delay variance factor. Simulation results indicate a throughput improvement over the default mechanism defined in RFC2960, but it doesn't address the switchover delays caused by increasing RTT values in WLAN environment.

Other studies investigate how the SCTP based switchover strategies can be enhanced. In fact, a pre-emptive 802.21 oriented switchover strategy based on signal strength is proposed in [3]. According to experimental results, authors prove that the new strategy behaves more effectively than standard reactive SCTP switchover strategy, since the 802.21 standard has the ability to predict network state changes.

In [4], authors analyze the traditional failover time estimation formula in wireless networking scenarios and expose its drawbacks. Then, they propose some updates to the SCTP failover strategy in order to more accurately reflect the exact time at which primary path failure occurs.

In [5], authors propose a cross layer algorithm which uses 802.11 MAC retransmissions as an indicator of performance for all paths within an association. The use of 802.11 MAC retransmissions permit to accurately predict this performance transition significantly earlier than at the transport layer.

In [6], a cross layer approach is presented in order to manage mobility in wireless environment. It introduces local, wireless and Internet RTO subcomponents which are combined to calculate end to end RTO. It also implements a decision mechanism which selectively implements backoff on RTO subcomponents depending on network conditions.

## III. CURRENT SCTP PATH MANAGEMENT

One of the features of SCTP that differentiates it from both TCP and UDP is its support of multi-homing which is the ability to support many IP addresses within an association. Multi-homing feature is used by SCTP to add resilience to network failures by providing a certain degree of network stability to critical transmission paths.

As a multi-homed protocol, SCTP needs a path management functionality to take switchover decisions as well as implementing the path switchover. To detect path failure, SCTP provides two kinds of probing mechanisms one for the primary path and another for the alternate paths. To monitor the primary path, SCTP keeps an error counter that counts the number of consecutive timeouts. For the alternate paths, SCTP uses a heartbeat mechanism to monitor the availability of these paths.

The SCTP path management functionality defines two states for each path. The state value can be set to ACTIVE or INACTIVE. A primary path is set to INACTIVE if transmission of packets on the path repeatedly fails. However, a secondary path fails, if a heartbeat chunk transmitted to the destination on that path was not successfully acknowledged. Both of these mechanisms are reactionary to network failure.

### A. Path Monitoring

In SCTP associations, secondary paths are monitored to detect any changes in the reachable state of a destination address, and also to update the Round Trip Time (RTT) measurement for each of these secondary addresses. Path monitoring is performed using HEARTBEAT chunks which are sent periodically to know which addresses defined in the association are reachable (see Figure 1). When a heartbeat is received by an endpoint, the packet is processed and a heartbeat ACK packet is sent back. Each heartbeat packet contains a timestamp of when it was sent. When the heartbeat ACK packet is received, the time delay difference can be used to estimate the Round Trip Round (RTT) for secondary paths.

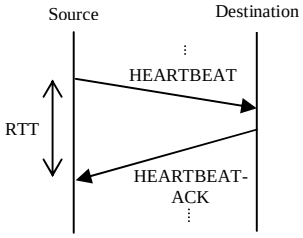



Figure 1. Secondary path monitoring

### B. Retransmission Timeout Calculation

In order to detect the primary path failure, SCTP uses a reactive strategy which is mainly based on a retransmission timer. The duration of this timer is referred to as RTO (Retransmission TimeOut) [7]. The RTO duration represents the delay between each retransmission on the path. The computation and management of RTO in SCTP is similar to how TCP manages its retransmission timer. However, SCTP differs from TCP by supporting multi-homing feature. In fact, when the destination is multi-homed, the endpoint will calculate a separate RTO for each different destination's transport address.

The RTO value of the primary path is important for path switchover decision. If an SCTP sender doesn't receive a response for an SCTP data chunk from its receiver within the time of Retransmission Timeout (RTO), the sender will consider this data chunk lost. When the number of consecutive timeouts on the primary path exceeds the SCTP threshold, the address will be marked as INACTIVE by the sender, and a new primary path will be selected among the alternate paths that are currently available.

 ISBN:978-1-61208-002-4 

The SCTP parameters which are used to implement the switchover management strategy are:

- RTO.Initial: the initial value for RTO.
- RTO.Min: the minimum time for RTO.
- RTO.Max: the maximum time for RTO.
- Path.Max.Retrans: the path retransmission threshold (PMR).
- HB.interval: the interval at which heartbeats are sent to monitor an SCTP endpoint.

According to [7], the following protocol parameters are recommended:

TABLE I. SCTP PARAMETERS FOR RTO CALCULATION

| Parameter | Recommended Value |
|---|---|
| RTO.Initial | 3 seconds |
| RTO.Min | 1 second |
| RTO.Max | 60 seconds |
| Path.Max.Retrans | 5 attempts |
| HB.interval | 30 seconds |

The retransmission Timeout (RTO) is calculated for each destination address separately based on the Smoothed Round Trip Time (SRTT) and Round Trip Time Variation (RTTVAR) of the path. SRTT and RTTVAR are calculated by the measurement of Round Trip Time (RTT) of the path. Initially RTO gets RTO.initial. Then, when SCTP gets the first measurement of RTT (RTT.1st), SRTT and RTTVAR are initialized as follow:

$$SRTT = RTT.1st \quad (1)$$

$$RTTVAR = RTT.1st / 2 \quad (2)$$

And RTO is updated to:

$$RTO = SRTT + 4*RTTVAR \quad (3)$$

For each time SCTP gets a new measurement of RTT (RTT.new), SRTT and RTTVAR will be updated as follow:

$$RTTVAR.new = (1-\beta)*RTTVAR.old + \beta*(SRTT.old - RTT.new) \quad (4)$$

$$SRTT.new = (1-\alpha)*SRTT.old + \alpha*RTT.new \quad (5)$$

Where α, the smoothing factor, and β, the delay variance factor, are constants and their recommended values are 1/4 and 1/8 respectively.

Then, the new RTO is:

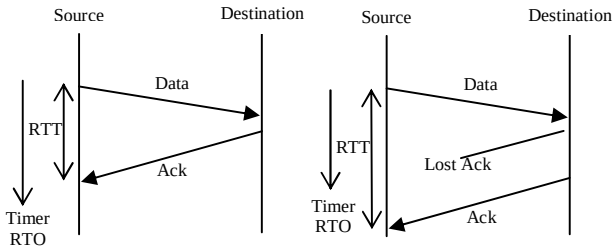
$$RTO = SRTT.new + 4*RTTVAR.new \quad (6)$$

If the new RTO is less than RTO.Min, it will be set to RTO.Min. If the new RTO is greater than RTO.Max, it will be set to RTO.Max.

Every time a transmission timeout occurs for an address (Figure 2(b)), the RTO for this address will be doubled (Backoff the time):

$$RTO = RTO \times 2 \quad (7)$$

As illustrated in Figure 2(a), if the sender gets a response from the receiver, a new RTT is measured. SCTP will use this new RTT to calculate RTTVAR, SRTT and finally RTO by the equations (4) (5) and (6).




(a) Transmission Success (b) Transmission Failure

Figure 2. Standard Path Failure Detection Strategy

### C. The Standard Path Failure Detection

The standard SCTP path failure detection strategy, as illustrated in Figure 3, is based on the retransmission timer with its managing rules as defined in RFC 2960 [7].

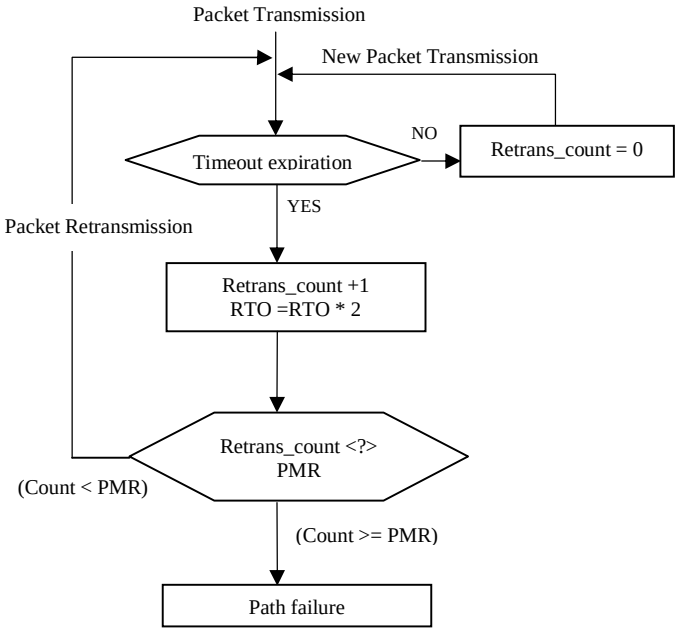



Figure 3. Standard Path Failure Detection Strategy

In fact, in SCTP association, packet transmission is through primary path only; other paths are back up in association. When a primary path is selected, the SCTP mechanism will mark the path to ACTIVE and use a retransmission count parameter to monitor path condition. If the timer expires, and the data chunk has not been acknowledged yet, it is assumed that the chunk is lost. Consequently, the actual RTO value for the affected path is doubled (exponential back-off mechanism), the error count is incremented by one and the lost chunk is marked for retransmission. When the retransmission count parameter reaches the threshold PMR (Path.Max.Retrans), the primary path takes failure. Then, the SCTP mechanism will change primary path state to INACTIVE and switch to a secondary path to continue transmission.

 ISBN:978-1-61208-002-4 

## IV. PROPOSED ALTERATION OF SCTP SWITCHOVER MECHANISM

Based on the sum of the consecutive retransmission timeouts, the standard strategy used by SCTP to detect the path failure is very simple and can't effectively distinguish path condition in wireless network. Consequently, this strategy is not always appropriate, especially when considering the SCTP multi-homing feature as a basis for achieving transport layer mobility in wireless network, where the transition time between available paths becomes a key aspect for the optimization.

Therefore, the most crucial challenge for SCTP is to provide optimal path management, aiming at improving the performance of the original switchover mechanism presented in Section III.

In this paper, we propose an improvement of the standard path failure detection strategy used by SCTP by changing the criteria of switchover initiation in order to obtain a more accurate estimation of the exact time at which primary path failure occurs (the Failover time). The alteration that we propose does not concern the formula of calculation of the parameter RTO. But it consist in defining new QoS parameters to preempt the path failure, and fixing thresholds to these parameters according to the type of traffic emitted and its requirements in terms of quality of service.

In fact, we propose to evaluate the Total Time spent expecting an acknowledgment ($T_{ack}$) in any case (packet transmission success or failure), which is an excellent indicator of path performance. $T_{ack}$ is computed by equation (8), by representing the sum of the (k-1) consecutive timeouts according to the RTO value at the transmission failure instant. However, if the packet sent is acquitted after (k-1) retransmission attempts, $T_{ack}$ is calculated by applying equation (9). The value (k-1) represents the number of retransmission attempts which is necessarily less than PMR ($0 < k \leq PMR$). The index j refers to the traffic type.

The time $T_{ack}$ will be the most important parameter to consider in the SCTP switchover decision. SCTP will use it as a path performance indicator to preempt degradation in path status and avoid service interruption.

In case of (k) failed attempts

$$T_{Ack,\,j} = \sum_{i=0}^{k-1} N_j^i * RTO$$

After simplification:

$$T_{Ack,\,j} = RTO * \frac{(1 - N_j^k)}{(1 - N_j)} \qquad (8)$$

In case of success after (k-1) failed attempts:

$$T_{Ack,\,j} = RTT_{success} + \sum_{i=0}^{k-2} N_j^i * RTO$$

After simplification:

$$T_{Ack,\,j} = RTT_{success} + RTO * \frac{(1 - N_j^{k-1})}{(1 - N_j)} \qquad (9)$$

We have also introduced a new condition to evaluate the path state depending on the time $T_{Ack}$ and the configured threshold for each type of traffic:

If $(T_{Ack,\,j} \geq T_{Threshold,\,j})$ Then (Primary path is INACTIVE)

Thus, the path is marked "INACTIVE" if one of the following conditions is satisfied:

- The number of retransmission timeouts reaches the maximum number of retransmission (PMR) authorized by SCTP.
- The waiting time $T_{ack}$ exceeds the threshold fixed for each type of traffic (VoIP, streaming video, data)

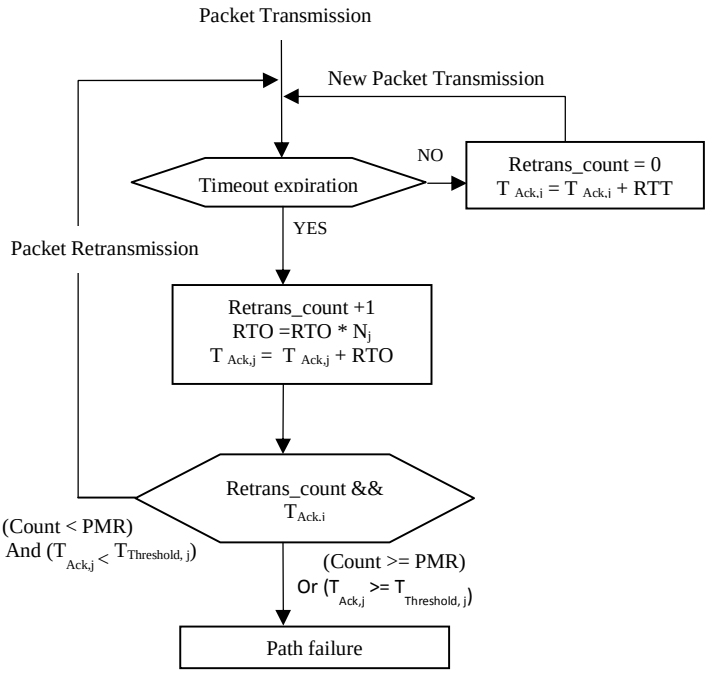



Figure 4. New Path Failure Detection Strategy

The modifications proposed with regard to the standard mechanism will be represented on the organization chart above (see Figure 4).

In RFC2960, the failure of packet retransmission induces the multiplication of the value of RTO by 2. As applications have different needs in terms of quality of service, we suggest penalizing the transmission failures in a different way for every type of traffic.

For real time streaming multimedia applications, such as voice over IP, which are delay sensitive, high latency can cause service quality degradation. However, Best effort traffic is more tolerant to delay. For these reasons, we propose to treat traffic flow differently by providing priority to certain flow, depending on their QoS requirements. We call $N_j$ the parameter used to penalize retransmission failure, where the index j indicates the traffic type. In RFC2960, this parameter is invariable and equal to 2.

In this work, we consider the followings values:

 ISBN:978-1-61208-002-4 

TABLE II. SCTP PENALIZING PARAMETERS

| Traffic Type | $N_i$ |
|---|---|
| Best Effort | 2 |
| VoIP | 1 |
| Video streaming | 1.25 |

## V. SIMULATION RESULTS

In order to illustrate the deficiencies of the strategy used by SCTP to detect the path failure and implement our proposed approach, we consider a network topology consisting of two base stations 802.11b and two nodes. The nodes are communicating and each one belongs to a base station. The network topology is shown in Figure 5.

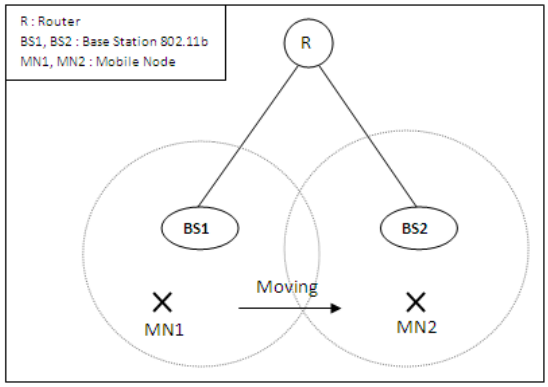



Figure 5. Simulated Network Topology

During simulation, we are interested to real-time traffics which are delay sensitive such as VoIP and video streaming. The video streaming traffic is simulated by an application that generates one packet every 26 milliseconds. Each packet has a size of 660 bytes. While the VoIP traffic is simulated by an application that generates packets of 160 bytes every 20 milliseconds. The traffic flow parameters are shown in Table 3.

TABLE III. SIMULATION TRAFFIC PARAMETERS

| Traffic | Delay Interval | Packet Size | Data Rate |
|---|---|---|---|
| VoIP | 20 ms | 160 bytes | 64 kb/s |
| Video | 26 ms | 660 bytes | 200 kb/s |

The simulation process time is 50 seconds, and all nodes start their transmission at 2s after the beginning of simulation time. Mobile node starts moving at 10s with a speed of 1m/s.

The simulation results presented in this paper were obtained using the network simulator NS2 [8] and the SCTP patch [9].

TABLE IV. SIMULATION PARAMETERS

| | |
|---|---|
| Simulation Time | 50 s |
| Trafic Start Time | 2 s |
| Trafic Stop Time | 50 s |
| Move Start Time | 10 s |
| Move speed | 1m/s |

We will first simulate the service differentiation module of our approach which consists in penalizing transmission's failures in a different way according to traffic type.

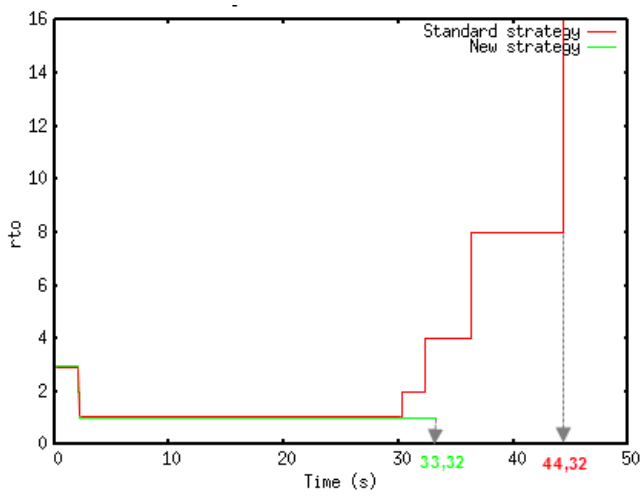



Figure 6. RTO values and Failover time detection for VoIP Traffic

Figure 6 and 7 illustrate respectively the RTO values for the simulated scenario for VoIP and video streaming traffic. When the mobile node moves away from the coverage area of the access point, signal strength degrades and the RTT and RTO increase. From simulation's result, we notice that SCTP take 15s to mark the destination address INACTIVE (T=1+2+4+8=15s). Which means that it would take 15s seconds for switchover to occur.

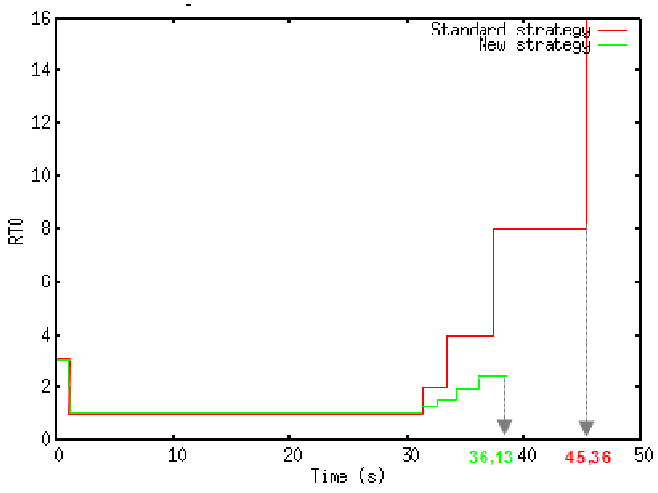



Figure 7. RTO values and Failover time detection for Video Streaming Traffic

 ISBN:978-1-61208-002-4 

The failover time is defined as the instant at which the primary path failure is detected. It is computed according to RTO values and corresponds to the (PMR-1) failed attempts to retransmit a lost chunk. Table 5 represents the failover instants for VoIP and Video streaming traffic when using the standard and the new SCTP path failure detection strategy. In fact, using the standard strategy, path failover is detected at 44,32s for VoIP and 45,36s for video streaming traffic. However, when using the new strategy based on service differentiation, the path failure is detected earlier at 33,32s for VoIP and 36,13s for video streaming traffic.

TABLE V. FAILOVER TIME FOR REAL TIME TRAFFIC

| Path Failure Detection Strategy | VoIP | Video Streaming |
|---|---|---|
| Standard strategy | 44,32s | 45,36s |
| Proposed strategy | 33,32s | 36,13s |

In our proposed approach, we defined a second condition to detect primary path failure which is based on delay $T_{ack}$ (Time spent expecting an acknowledgment). Figures 8(a) and 8(b) represents $T_{ack}$ values for respectively VoIP and Video Streaming traffic. This parameter reflects the link state and therefore it can be considered to predict network performance degradation. Thus, $T_{ack}$ will be a decisive parameter to initiate switchover process.

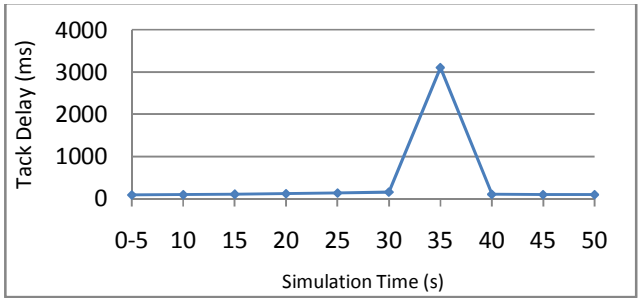



Figure 8-(a) $T_{ack}$ Delay for VoIP Traffic

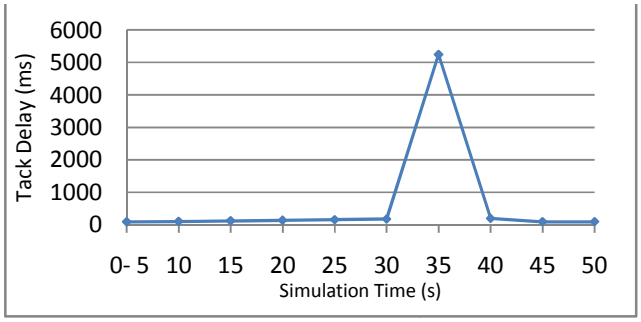



Figure 8-(b) $T_{ack}$ Delay for Video Streaming Traffic

Figure 8. $T_{ack}$ Delay for for Real Time Traffic

To further illustrate the shortcomings of the standard method and highlight the contribution of our new approach to detect primary path failure, we will represent network's performance metrics such as throughput, delay and loss.

1) Throughput

The throughput, measured in kbps, corresponds to the amount of data in bits that is transmitted over the channel per unit time.

$$Throughput = \frac{Total\ number\ of\ bits\ successfully\ transmitted\ during\ T}{T}$$

2) End-to-End Delay

The end to end delay, measured in second, is the time taken for a packet to be transmitted across a network from source to destination. It is an important parameter to evaluate the QoS for the real-time traffic.

$$Delay = \frac{\sum_{i=0}^{N} (Time\ of\ packet_i\ received\ -\ Time\ of\ packet_i\ sent)}{Total\ number\ of\ packet\ received}$$

3) Packet Loss Rate

Packet loss is expressed as a percentage of the number of packets lost to the total number of packets sent.

$$Packet\ Loss\ Rate = \frac{Number\ of\ dropped\ data\ packet}{Total\ number\ of\ packet\ data\ sent} \times 100$$

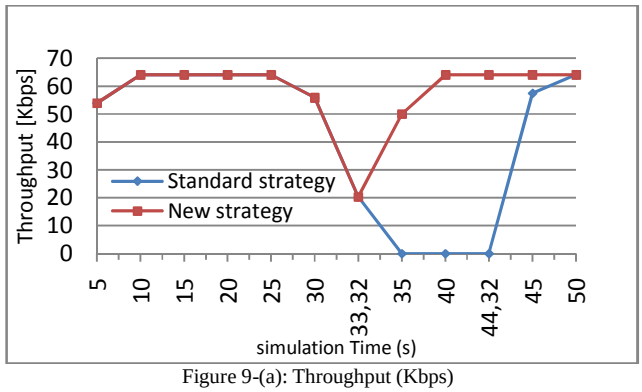



Figure 9-(a): Throughput (Kbps)

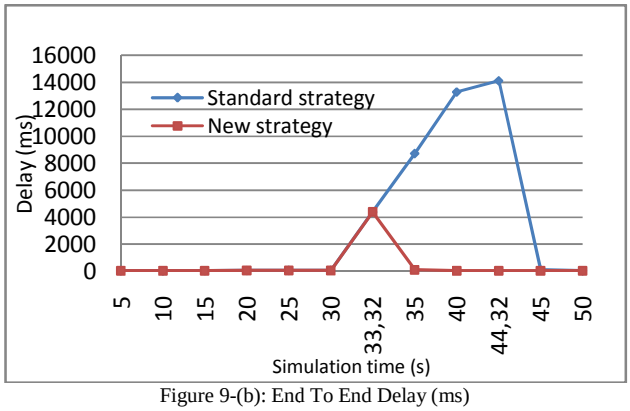



Figure 9-(b): End To End Delay (ms)

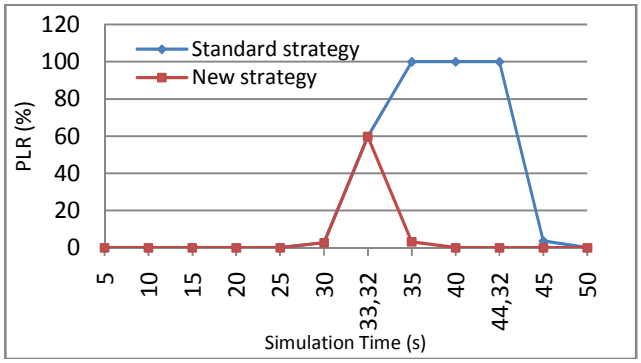



Figure 9-(c): Packet Loss Rate

Figure 9. Performance metrics for VoIP traffic

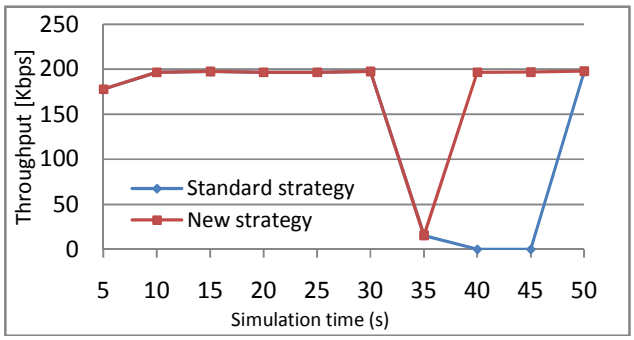



Figure 10-(a): Throughput (Kbps)

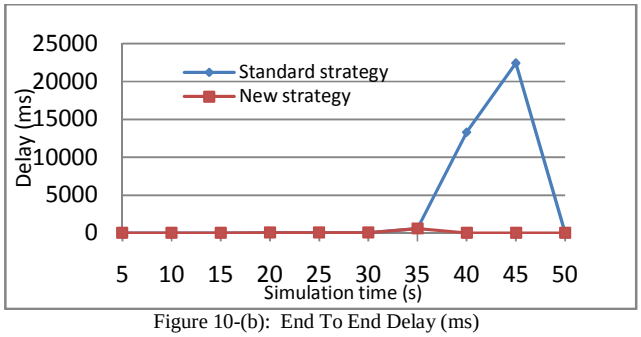



Figure 10-(b): End To End Delay (ms)

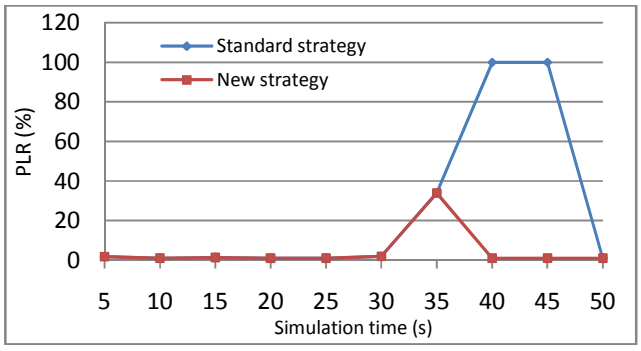



Figure 10-(c): Packet Loss Rate

Figure 10. Performance metrics for Video Streaming traffic

Figures 9 and 10 represent the metrics of network performance (Throughput, Delay and Packet loss) for respectively VoIP and Video streaming traffic. According to simulation's result, we notice that when using the standard strategy, although there was a degradation of network performance in terms of throughput, delay and loss, SCTP delays switchover, i.e., SCTP allows more time to initiate switchover.

Through simulation results, we deduce that our approach could be an alternative to the current SCTP path failure detection strategy used by SCTP; by increasing network performance and providing a seamless switchover to real-time applications such as VoIP or video streaming

## VI. CONCLUSION

In this paper, we are interested to the mechanism used by SCTP to take the decision of changing the primary path which relies mainly on the failover mechanism. We have detailed the current mechanism implemented in SCTP and described some of its failings. Then, we have proposed a proactive approach to detect the path failure. Our approach would be more suitable to a mobile environment such as WLAN. In fact, according to experiment results, the proposed approach allows SCTP to detect the path failover earlier than the standard mechanism. Moreover, it provides a seamless switchover to real-time applications by increasing network performance and avoiding service interruption. In future work, we will investigate the algorithm used by SCTP to estimate the RTO timer, in order to enhance switchover performance in WLAN environment.

## REFERENCES

[1] S. Fallon, P. Jacob, Y. Qiao, and L. Murphy, "SCTP Switchover Performance Issues in WLAN Environments", 5th IEEE Consumer Communications and Networking Conference (CCNC) 2008, Issue 10- 12 Jan. 2008, pp. 564 – 568

[2] S. Fallon, P. Jacob, Y. Qiao, and L. Murphy, "An Analysis of Alterations to the SCTP RTO Calculation Mechanism for WLAN Environments". In MWCN 2008 Wireless and Mobile Networking. IFIP, vol. 284, pp. 95–108 (2008)

[3] E. Fallon, J. Murphy, L. Murphy, Y. Qiao, X. Xie, and A. Hanley, " Towards a Media Independent Handover Based Approch to Heterogenous Network Mobility", In Proceedings of The IET Irish Signals and Systems Conference 2007 (ISSC07).

[4] L. Budzisz, R. Ferrus, K. Grinnemo, A. Brunstrom, and C. Ferran, "An Analytical Estimation of the Failover Time in SCTP Multihoming Scenarios", Wireless Communications and Networking Conference (WCNC) 2007.

[5] S. Fallon, P. Jacob, Y. Qiao, A. Hanley, and L. Murphy, "Using 802.11 MAC Retransmissions for Path Selection in Multi-homed Transport Layer Protocols". In Proceedings of the IEEE Global Communications Conference (GLOBECOM 09).

[6] S. Fallon, P. Jacob, Y. Qiao, and L. Murphy, "An Adaptive Optimized RTO Algorithm for Multi-homed Wireless Environments", 7th International Conference on Wired and Wireless Communications (WWIC) LNCS 5546, pp. 133-145 (2009)

[7] R. Stewart, Q. Xie, K. Morneault, C. Sharp, and H. Schwarzbauer, T.Taylor, I.Rytina, M.Kalla, L.Zhang, V. Paxson. "RFC2960 - Stream Control Transmission Protocol ".October 2000.

[8] Network Simulator- NS2- http://www.isi.edu/nsnam/ns.

[9] SCTP Patch for NS. http://pel.cis.udel.edu.

 ISBN:978-1-61208-002-4 