RESEARCH ARTICLE OPEN ACCESS

Performance Analysis of TCP and SCTP For Congestion Losses In Manet

Er.Amritpal Kaur[*], Er.Pooja Rani[**]
[*](Mtech.Scholar, Department of CSE, RBIEBT, Mohali Campus, Tehsil-Kharar, Punjab-140104)
[**](Associate Professor, Department of IT, RBIEBT, Mohali Campus,Tehsil-Kharar, Punjab-140104)

ABSTRACT-
Transmission control protocols have been used for data transmission process. TCP has been pre-owned for data transmission over wired communication having different bandwidths and message delays over the network. TCP provides communication using 3-handshake which sends RTS and ACK comes from server end and data message has been transmitted over the bandwidth provided. This does not provide security over flooding attack occurred on the network. TCP provides communication between different nodes of the wired communication but when multi-streaming occurs in a network TCP does not provides proper throughput of the system which is major problem that occurred in the previous system. In the proposed work, to overcome this problem SCTP transmission control protocol has been implemented for the system performance of the system. SCTP provides 4-handshake communication in the message transmit due to which security factor get increases and this also provides communication services over multi-streaming and multi-homing. Multiple sender and receivers can communicate over wired network using various approaches of communication through same routers, which degrades in the TCP protocol. In final we evaluate parameters for performance evaluation. Here, we designed and implemented our test bed using Network Simulator (NS-2.35) to test the performance of both Routing protocols.
Keywords-MANET, Delay, PDR, SCTP, TCP, Throughput, Loss rate

I. INTRODUCTION

1.1 MANET

A versatile specially appointed system (MANET) is a persistently self-arranging, foundation less system of cell phones joined without wires. Specially appointed is Latin and signifies "for this reason". In a MANET each widget is involved in go without reliance in any bearing [14], and will consequently change its connections to different gadgets much of the time. The principle challenge in building a MANET is preparing every gadget to ceaselessly keep up the data needed to legitimately course activity. Such systems may work independent from anyone else or may be joined with the bigger Internet. They may contain one or various and distinctive handsets between hubs. This results in an exceedingly alterable, self-ruling topology [16]. MANETs are a sort of Wireless impromptu system that more often than not has a routable systems administration environment on top of a Connection Layer impromptu system. MANETs comprise of a distributed [15], self-shaping, self-mending system as opposed to a lattice system has a focal controller (to focus, advance, and disseminate the directing table). MANETs around 2000-2015 commonly impart at radio frequencies (30 MHz - 5 GHz).Multi-jump transfers go back to no less than 500 BC. The development of tablets and 802.11/Wi-Fi remote systems administration has made MANETs a well known exploration subject subsequent to the mid-1990s. Numerous MANETs comprise of a distributed [15], self-shaping, self-mending system as opposed to a lattice system has a focal controller (to focus, advance, and disseminate the directing table).

MANETs around 2000-2015 commonly impart at radio frequencies (30 MHz - 5 GHz).Multi-jump transfers go back to no less than 500 BC. The development of tablets and 802.11/Wi-Fi remote systems administration has made MANETs a well known exploration subject subsequent to the mid-1990s. Several scholarly papers assess conventions and their capacities, expecting fluctuating degrees of versatility inside of a limited space, more often than not with all hubs inside of a couple jumps of one another.

Dissimilar protocols are then assessed taking into account measures, such as, the bundle drop rate, the transparency introduced by the routing protocol, end-to-end packet delay, system throughput, capacity to scale, and so forth [16].

1.2 TYPES OF MANET:

- Vehicular Ad hoc Networks (VANETs) are utilized for correspondence among vehicles and in the middle of vehicles and roadside gear. Shrewd vehicular specially appointed systems (In VANETs) are a sort of computerized reasoning that helps vehicles to carry on in keen conduct amid vehicle-to-vehicle crashes, mishaps, inebriated driving and so forth [14].

- Smart Phone Ad hoc Networks (SPANs) leverage the existing equipment (primarily Bluetooth and Wi-Fi) in industrially accessible advanced mobile phones to make shared systems without depending on cell bearer systems, remote access focuses, or conventional system foundation. Compasses vary from conventional center point and talked systems, for example, Wi-Fi Direct, in that they bolster multi-bounce transfers and there is no thought of a gathering pioneer so associates can join and leave voluntarily without pulverizing the system [17].

- Internet based portable specially appointed systems (iMANETs) are impromptu systems that connection versatile hubs and altered Internet-entryway hubs. Case in point, different sub-MANETs may be joined by in a fantastic Hub-Spoke VPN to make a topographically appropriated MANET. In such sort of systems ordinary specially appointed directing calculations don't have any significant bearing specifically [14].

- Military/ Tactical MANETs are utilized by military units which laid on reach, incorporation and security with frameworks which as of now. Normal waveforms incorporate the US Army's SRW, Harris' ANW2 and HNW, Persistent Systems' Wave Relay, Trellis ware’s TSM and Silvus Technologies' Stream Caster [13].

- A mobile ad-hoc network (MANET) is an ad-hoc network but an ad-hoc network is not necessarily a MANNET.

1.3 CONGESTION IN MANET

In a system with shared assets, where numerous senders go after connection transfer speed, it is important to modify the information rate utilized by every sender as a part of request not to over-burden the system. Bundles that land at a switch and can't be sent are dropped, thusly an intemperate measure of parcels touching base at a system bottleneck prompts numerous parcel drops. These dropped parcels may as of now have voyage far in the system and hence expended significant assets. Moreover, the lost parcels regularly trigger retransmission which implies that significantly more bundles are sent into the system. Accordingly organize clogging can extremely fall apart system throughput. In the incident that no appropriate blockage control is performed this can prompt a blockage breakdown of the system, where no information is effectively conveyed. Such a circumstance happened on the early Internet, prompting the improvement of the TCP clogging control system [13].

II. TCP (Transmission Control Protocol) as wide area Network

TCP has been enhanced for wired systems. Any bundle misfortune is thought to be the aftereffect of system blockage and the clogging window size is lessened significantly as insurance [8]. On the other hand, remote connections are known not sporadic and typically interim misfortunes because of blurring, shadowing, hand off, and other radio impacts, that can't be considered blockage. After the (wrong) back-off of the blockage window size, because of remote bundle misfortune, there can be a clogging evasion stage with a progressive reduction in window size. This causes the radio connection to be underutilized. Broad examination has been done on the subject of how to battle these unsafe impacts. Proposed arrangements can be classified as end-to-end arrangements (which want modified changes at the client or server),link layer solutions, (such as RLP within cellular networks), or substitute based solutions(which necessitate some change in the network devoid of modifying the end nodes[7].

2.1 TCP RENO

TCP uses a multi-faceted congestion-control strategy to avoid congestion collapse, [6]. For each connection, TCP maintains a congestion window, ending with the total number of unacknowledged packets that may be in transit from end-to-end. This is somewhat similar to TCP's sliding window that is used for flow control. Basically TCP uses a mechanism called slow start to make the congestion window to a increase level after a connection is initialized and subsequent to a break. It start with a casement of two times the maximum segment size (MSS). Although the original rate is short, the speed of increase is incredibly speedy for every packet recognized, the clogging window increases via 1 MSS so that the congestion window effectively doubles for every round-trip time (RTT) [5]. The algorithm enters a new state When the congestion window exceeds a threshold, called congestion avoidance In some implementations (*e.g.*, Linux), the initial thresh is large, and so the first slow start usually ends after a loss. However, thresh is updated at the end of every slow beginning, and will frequently affect subsequent slow starts triggered by timeouts [9].

- **Congestion avoidance:** As long as there are non-duplicate ACKs received, the congestion window is additively increased by one MSS every round trip time [9]. When a packet is lost, the likelihood of duplicate ACKs being received is very high (it's possible though unlikely that the stream just underwent tremendous sachet reordering, which would also timely duplicate ACKs).

- **Reno:** If there are three duplicate ACKs established (i.e., there are four ACKs approving the identical packet, which are not piggybacked on the data, and do not change the receiver's advertised window), Reno will halve the congestion window (instead of setting it to 1 MSS alike to Tahoe), put the slow start threshold equivalent to the new clogging window, execute a speedy retransmit, and go through a phase called Fast Recovery [3].

- **Fast recovery:** In this state, basically TCP retransmits the lost packet that was signaled by three duplicate ACKs, and waits for the acknowledgment of the entire transmit window before going back to congestion avoidance [2]. If there is no acceptance, TCP Reno experiences a break as well as enters the slow-start state.

2.2 TCP New Reno

TCP New Reno now improves retransmission during the fast-recovery phase of TCP Reno. During fast recovery, each and every duplicate ACK that is returned to TCP New Reno, a new unrelieved packet from the end of the congestion casement is sending, to remain the broadcast window full. For each ACK with the aim to make partial progress in the succession space, the sender assume that the ACK points toward a original hole, and the subsequently packet beyond the ACKed sequence number is sent. As the timeout timer is reset whenever there is progress in the transmit buffer, this basically allows New Reno to plug great holes, or numerous holes, in the sequence space – much like TCP SACK [3]. Since New Reno can send new bundles toward the end of the clogging window amid fast recovery, higher throughput is achieved during the hole-filling procedure, even when there are frequent holes, with the number of packets each. TCP minutes the highest outstanding unacknowledged packet sequence number when it enters speedy recovery. TCP proceeds to the congestion prevention state when this sequence number is recognized. A problem occurs only with New Reno when there are no packets losses but incase; packets are reordered by more than 3 packet sequence numbers [4]. When this happens, New Reno sometimes enters fast recovery, however when the reordered packet is transported, ACK sequence-number development occurs and from there until the end of rapid healing, every small piece of sequence-number growth produces a copied and needless retransmission that is instantaneously ACK. New Reno performs as well as SACK at low packet blunder charges, and extensively outperforms Reno at prominent fault rates [6].

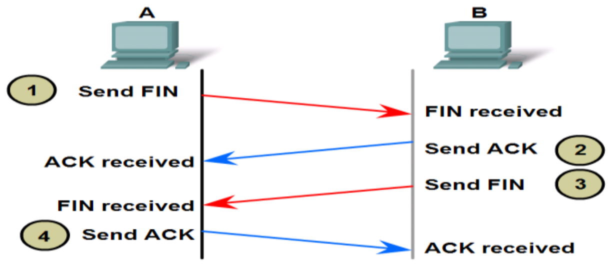

Fig 1: TCP Congestion Control

III. SCTP (Stream Control Transmission Protocol)

Stream Control Transmission Protocol (SCTP) is a transport layer protocol, which serve the corresponding task to the popular protocols i.e Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). It provides some of the identical overhaul features of both: it is message-oriented like UDP and ensure consistent, in-subsequence transfer of messages with congestion control like TCP. The protocol was distinct by the IETF Signaling Transport (SIGTRAN) functioning cluster in 2000, and is maintain by the IETF Transport Area (TSVWG) functioning cluster [12].
The term multi-streaming refers to the potential of SCTP to send out several autonomous streams of chunks in equivalent [11], for example transmitting web page metaphors jointly with the web page text. In real meaning, it associates bundling numerous associations into a single SCTP connection, in service on messages (or chunks) slightly than bytes.

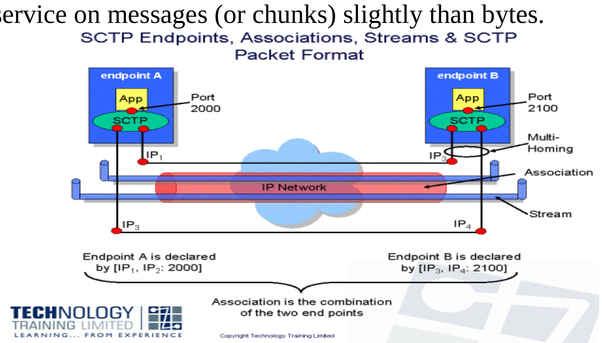

Fig 2: SCTP protocol

3.1 Message-based multi-streaming

SCTP applications present their information to be transmitted in messages (gatherings of bytes) to the SCTP transport layer. SCTP spots messages and control data into isolated pieces (information lumps and control lumps), each recognized by a piece header. The convention can section a message into various information pieces, yet every information piece contains information from stand out client message [12]. SCTP groups the lumps into SCTP parcels. The SCTP parcel, which is submitted to the Internet Protocol, comprises of a package header, SCTP control lumps (when required), and took later than by SCTP information pieces (when available) [11].

SCTP may be described as message-oriented, means that it delivers a succession of messages, somewhat than delivering a continuous stream of bytes as does TCP. As in UDP, in SCTP a sender assigns a message in one movement, and that the precise message is conceded to the receiving application progression in one movement.

In distinction, TCP is a current-oriented protocol, bringing streams of bytes constantly and in organized form. However TCP does not permit the receiver to identify how many times the sender application labeled on the TCP transport transiency it group the bytes to be sent out. At the sender, TCP merely append extra bytes to a row of bytes coming up to go out over the network, somewhat than having to maintain a lineup of particular split outbound messages which might be conserved as such [13].

The term multi-spilling alludes to the capacity of SCTP to transmit a few autonomous floods of lumps in parallel [11], for instance transmitting site page pictures together with the site page content. Fundamentally, it includes packaging a few associations into a solitary SCTP affiliation, working on messages (or lumps) instead of bytes.

TCP jelly byte arrange in the stream by allotting a succession number to every bundle. SCTP, then again, allocates an arrangement number to every message sent in a stream. This permits autonomous requesting of messages in diverse streams. In any case, message requesting is discretionary in SCTP; a getting application may decide to process messages in the request of receipt rather than the request they were sent [12].

3.2 FEATURES OF SCTP

- Multihoming backing in which one or both endpoints of an association can comprise of more than one IP location, empowering straightforward fall flat over between recurring system ways [14].
- Delivery of pieces inside of autonomous streams dispenses with pointless head-of-line obstructing, rather than TCP byte-stream conveyance.
- Path choice and observing select an essential information transmission way and test the network of the transmission way [11].
- Validation and affirmation components secure against flooding assaults and give notice of copied or missing information pieces.
- Improved blunder recognition suitable for Ethernet gigantic casings [14].

The originators of SCTP initially proposed it for the convey of telephony in excess of Internet Protocol, with the objective of copying a number of the reliability characteristics of the SS7 signaling network in IP.This IETF attempt is recognized as SIGTRAN.In the interim, other benefits have been designed, for instance, the distance protocol and Reliable serve.

FLOW OF WORK

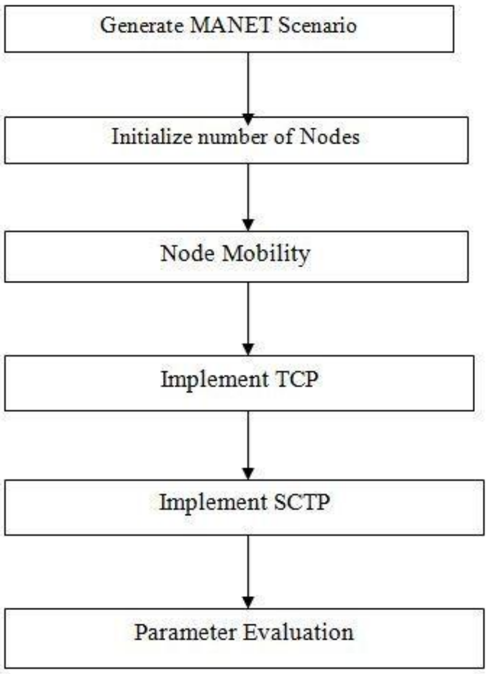

Fig 3: Flow of work

SIMULATION PARAMETERS:

The simulation parameter has shown in Table 1. At this point, we designed and implemented our test bed using Network Simulator (NS-2.35) to test the performance of both Routing protocols.The total simulation time is 140 second.

PARAMETER	VALUE
Simulation duration	140s
Topology area	1000 m x 1000 m
Number of nodes	20
Mobility model	Random way point
Transmission range	250 m
Packet rate	4 packets/s
Packet size	512 b

Table 1: Simulation Parameters

IV. RESULTS AND DISCUSSIONS

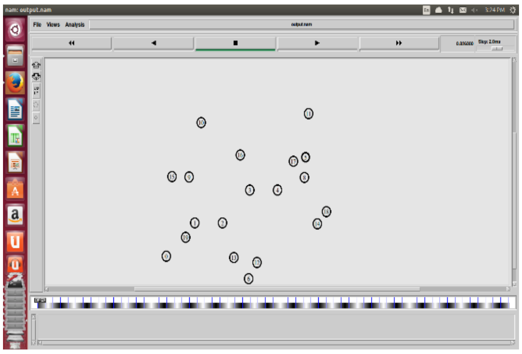

Fig 4: Representation of nodes

In this scenario the nodes take their respective positions.

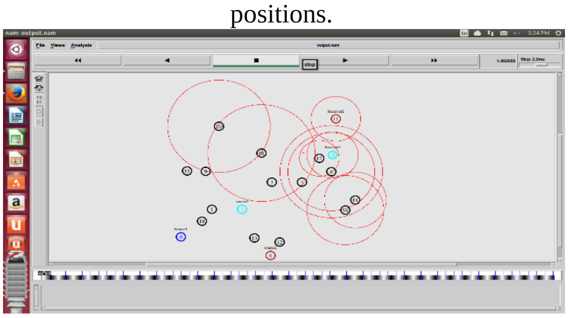

Fig 5: Representation of source and destination nodes

This figure represents number of nodes and number of destinations which will communicate with each other.

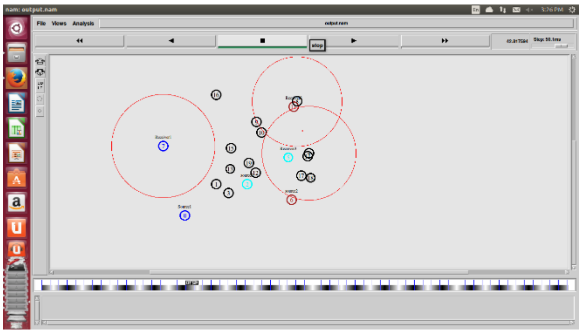

Fig 6: Representation of communication between the nodes

This scenario represents that the node which were later far away is now in communication with the other nodes.

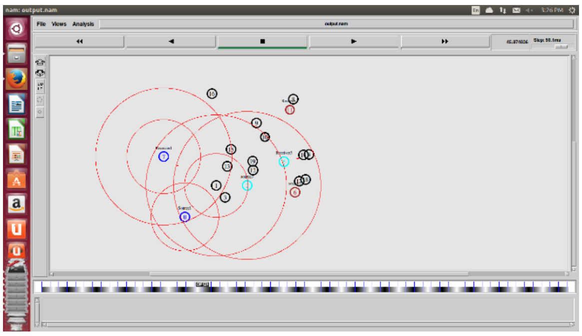

Fig 7: Representation of communication

In this figure all the nodes started communicating with each other.

In the graphs red color line represents SCTP and green color line represents TCP.

Fig 8: Represents PDR

This figure represents PDR (Packet delivery ratio). PDR with SCTP is better as compared to Without SCTP.

Fig 9: Represents throughput

Throughput is total number of successful bites received. This graph represents throughput.

Fig. 10: Represents delay

This figure represents end to end delay of nodes. With SCTP delay is lesser as compared to without SCTP hence, after applying SCTP result are better.

Fig 11: Represents Loss rate

This figure represents that loss rate in SCTP is negligible as compared to loss rate without SCTP.

V. RESULTS EVALUATION:

Parameters	Evaluation for TCP	Evaluation for SCTP
Average throughput	100.25 kbps	145.87 kbps
Average end to end delay	454.974m/s	93.0574m/s
Packet delivery ratio	81.1814%	93.7589%

Table 2: Results Evaluation

VI. CONCLUSION

TCP and SCTP are working on transport layer and they help in communication. SCTP is a four handshake scheme which also enhances the security of the system. In this work performance of TCP and SCTP is measured for Ad-hoc network and it has been analyzed that SCTP gives better result for all the network parameter as compare to TCP. Performance is measured on the basis of four parameters like throughput, delay, packet delivery ratio and loss. In the future we can implement this transmission protocol in real world example and by using different protocols for transmission in ADSL network, One can find out best routing protocol which provide maximum throughput for the system.

REFERENCES

[1] Narender Sharma; Rajesh Kumar Chakarwarti "Simulation for Congestion-Less Losses Control over MANET using TCP Scheme" IEEE 2014 International Conference on Issue and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, pp 410

[2] Maninder kaur,Parminder Singh, "A Mathematical Approach to Avoid Congestion and To Analyize Snoop Behaviour In Wired Cum Wireless Network", IJEAT, vol-2, issue 2, 2012, pp.347-352.

[3] Shiying Lei, "Performance of TCP in Intermittently Connected Wireless Networks: Analysis and Improvement", IEEE, 2010.

[4] Niels Mollar, "Inter-Protocol fairness between TCP New Reno and TCP Westwood", Route des Lucioles, 2004..Ait-Hellal, "Analysis of TCP Reno and TCP New Reno", 1990.

[5] Afiqah Azahari, "Review of Error Detection of Data Link Layer in Computer network, IDOSI Publications, 2013.

[6] Bestavros, A "TCP Boston: a fragmentation-tolerant TCP protocol for ATM networks", ISSN 0-8186-7780-5, PP 1210 – 1217, vol. 3, IEEE, 1997

[7] Ke Liu "Impact of TCP protocol efficiency on mobile network capacity loss", ISSN 978-1-61284-824-2, pp. 1 – 6, IEEE, 2013.

[8] whee Joe "An Enhanced TCP Protocol for Wired/Wireless Networks", ISSN 531 – 533, PP 428 – 433, IEEE, 2008.

[9] Tropea, M. "A new TCP Bandwidth Estimation protocol for satellite networks", ISSN 978-1-4673-2479-3, pp. 13 – 18, 2013.

[10] Jun Ke "Towards a rate-based TCP protocol for the Web", ISSN 0-7695-0728-X, PP 36 – 45, IEEE, 2000.

[11] Pfutzenreuter, "Performance Evaluation of SCTP Protocol in Linux", ISSN 1548-0992, PP 170 – 175, IEEE, 20007.

[12] Boussen, S. "Performance Analysis of SCTP Protocol in WiFi Network" , ISSN 978-1-4244-5244-6, PP 178 – 182, IEEE, 2009.

[13] Filho, E.L "A High Availability Firewall Model Based on SCTP Protocol", ISSN 978-0-7695-3371-1, PP 202 – 207, IEEE, 2008.

[14] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing" In *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, Vol. 3, pp. 90–100, Feb. 1999.

[15] Danai Chasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in Secure MANET" in *Military Communications Conference, 2009. MILCOM 2009. IEEE* Vol.2, Issue 2, pp. 1-6.

[16] H. Tian and H. Shen, "Multicast-based inference of network-internal loss performance," in *Proc. of 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN 2004)*, Hong Kong, China, Vol.6 pp. 288–293.

[17] Kartik Kumar Srivastava, Avinash Tripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" in *International journal Computer Technology & Applications Dec 2003,Vol.3, Issue 6*, pp. 1915-1921.