Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Research on Comparison of TCP and SCTP over MANET'S

Rajbir Kaur
Dept of Computer Science Engg.,
Mtech Full Time RIMT IET, Punjab India

Rupinder Kaur Gurm
Assistant Professor of Dept of Computer Science Engg, RIMT IET, Punjab, India

Abstract- A mobile ad-hoc network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a Mobile Ad-hoc Network usually seek the help of other intermediate nodes to establish communication channels. A Mobile Ad-hoc Network is a group of wireless mobile computers in which nodes cooperate by forwarding packets for each other to allow them to communicate. TCP has been used for data transmission communication having different bandwidths and message delays over the network. This does not provide security over flooding attack occurred on the network. TCP provides communication between different nodes 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. To overcome this problem SCTP transmission control protocol has been used for the system performance of the system. SCTP provides 4-way 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. We compare performance metrics between TCP & SCTP such as packet delivery ratio, throughput, end-to-end delay, packet loss and energy are evaluated using NS-2 based simulations and results shows better performance.

Keywords: MANET, TCP, SCTP, LEACH, AODV.

I. INTRODUCTION

1.1 MANET

MANET is called Mobile Ad hoc Networks. Mobile implies "mobility". Ad hoc is a Latin word that means "for this only". MANET is an autonomous collection of mobile nodes that communicate over wireless links. MANET is a minimum IP based network of mobile and wireless machine nodes connected with radio. In operation, the nodes of a MANET do not have a centralized administration mechanism. It is known for its route network properties where each node act as a "router" to forward the traffic to other specified node in the network. In MANET nodes moves randomly and organize themselves arbitrarily. The nodes directly communicate via wireless links with each other's radio range, while that are distant apart use other nodes as relay, in a multi-hop routing function. Ad hoc networks are self-configuring and self-organizing, so to maintain communication between nodes in the network, each node behaves as a source, start point, a host and a router. "A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links."

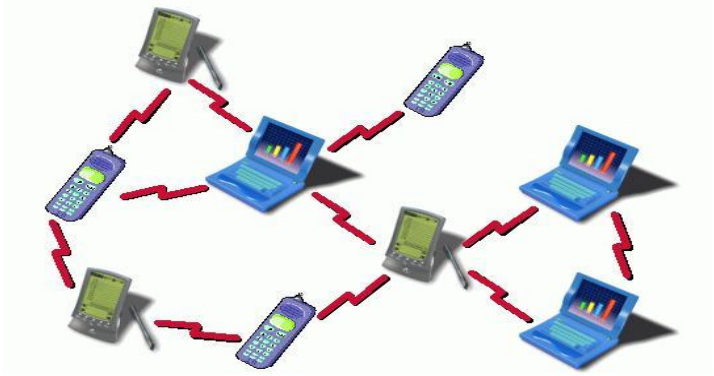


Fig 1: MANET

Some of the main features of MANET are listed below:

- MANET can be formed without any pre-existing infrastructure.
- It work on dynamic topology where nodes may join and leave the network at any time with their own choice and the multi-hop routing may keep changing as nodes join and depart from the network.
- It does have very limited physical security, and thus increasing security is a major concern.
- Every node in the MANET can assist in routing of packets in the network.
- Both Bandwidth & Power in limit.

1.2 Types of MANET

- Vehicular Ad hoc Networks (VANETs) are used also in communication. Communication among vehicles and between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (In VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving with phone calls.
- Internet based mobile ad hoc networks (I MANETs) are ad hoc networks that link mobile nodes. Fixed Internet-gateway nodes. For example, multiple sub-MANETs may be connected by in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms don't apply directly.
- Military MANETs are used by military units with emphasis on security, range, and integration with existing systems. Common waveforms include the US, Persistent Systems' Wave Relay, and Trellis ware's TSM.

1.3 Challenges in MANET

A MANET environment has to overcome certain issues of limitation and inefficiency. It consists of following:

- The characteristics of wireless link are time-varying in nature.

There are transmission barrier like path loss, blockage and interference that adds to the susceptible behavior of wireless channels. The dependability of wireless transmission is resisted by different factors.

- Limited range of wireless transmission

The limited radio band results in reduced data rates compared to the wireless networks. Hence best usage of bandwidth is necessary by keeping low overhead as possible.

- Packet losses due to errors in transmission

MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high bit error rate (BER)), interference, and frequent breakage in paths caused by mobility of nodes, increased collisions due to the presence of hidden terminals and unidirectional links.

- Route changes due to mobility

The dynamic network topology results in frequent path breaks.

- Frequent network partitions

The random movement of nodes often leads to partition of the network. This always affects the intermediate nodes

1.4 Applications of MANET

Some of the typical applications include:

- Military battlefield

Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter

- Collaborative work

For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

- Local level

Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

- Personal area network and Bluetooth

A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the intercommunication between various mobile devices such as a laptop, and a mobile phone.

- Commercial Sector

Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where none existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

1.5 Techniques Used

Transmission Control Protocol (TCP)

TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet. TCP is defined by the Internet Engineering Task Force (IETF) in the Request for Comment (RFC) standards. TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control, and because it is meant to provide error-free data transmission handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive. In the Open Systems Interconnection (OSI) communication model, TCP covers parts of Layer 4, the Transport Layer, and parts of Layer 5, the Layer 3.

SCTP (Stream Control Transmission Protocol)

Stream Control Transmission Protocol (SCTP) is a transport layer protocol (protocol number 132), serving in a similar role to the popular protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). It provides some of the same service features of both: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP. The protocol was defined by the IETF Signaling Transport working group in 2000, and is maintained by the IETF Transport Area (TSVWG) working group.

Message-based multi-streaming

SCTP applications submit their data to be transmitted in messages (groups of bytes) to the SCTP transport layer. SCTP places messages and control information into separate chunks (data chunks and control chunks), each identified by a chunk header. The protocol can fragment a message into a number of data chunks, but each data chunk contains data from only one user message. SCTP bundles the chunks into SCTP packets. The SCTP packet, which is submitted to the Internet Protocol, consists of a packet header, SCTP control chunks (when necessary), and followed by SCTP data chunks (when available) .

Features of SCTP

- Multi homing support in which one or both endpoints of a connection can consist of more than one IP address, enabling transparent fail-over between redundant network paths.
- Delivery of chunks within independent streams eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.
- Path selection and monitoring select a primary data transmission path and test the connectivity of the transmission path.
- Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks.
- Improved error detection suitable for Ethernet jumbo frames.

II. PROTOCOL USED

- **LEACH**

Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC protocol which is integrated with clustering and a simple routing protocol in wireless sensor networks (WSNs). The goal of LEACH is to lower the energy consumption required to create and maintain clusters in order to improve the life time of a wireless sensor network. LEACH is a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station (sink). Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round. LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head, but that using this radio at full power all the time would waste energy. Nodes that have been cluster heads cannot become cluster heads again for P rounds, where P is the desired percentage of cluster heads. Thereafter, each node has a 1/P probability of becoming a cluster head in each round. At the end of each round, each node that is not a cluster head selects the closest cluster head and joins that cluster. The cluster head then creates a schedule for each node in its cluster to transmit its data.

- **AODV (Routing Protocol)**

The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced. A disadvantage is a possible large delay from the moment the route is needed (a packet is ready to be sent) until the time the route is actually acquired. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time.

III. RELATED WORK

Maninder Kaur, Parminder Singh [1] describes that performance of the TCP (Transmission Control Protocol) has been promising in case of wired networks. In wireless network the packet loss is not only due to congestion but to be also due to high bit error rates and hand offs .Also improving its performance in wired-cum-wireless networks preserving the end-to-end nature of TCP is a difficult task. To address this issue, several new protocols and TCP modifications such as Snoop have been proposed. Usually problems faced by TCP when it works in wireless networks and this is the reason Snoop protocol is a better solution for this problem because it introduces a Snoop agent at the base station, which monitors packets flowing in both directions. The most well known TCP-aware link layer recovery scheme is the Snoop Protocol. It maintains a cache of the packets and whenever a packet loss is detected, it does a local recovery and drops all duplicate acknowledgements.

Shiying Lei, ET. al. [2] It describes about the ICWN i.e. Intermittently Connected Wireless Networks especially when Epidemic Routing is used to evaluate the performance or Delay/disruption Tolerant Networks (DTN), have attracted attention from researchers because of their inherent characteristics including long latency, low data rate and intermittent connectivity. It also shows that Epidemic Routing in ICWN degrades the performance of TCP because multi-copy data packets cause duplicate ACK's , and in turn reduce the transmitting rate of TCP. Then an enhanced algorithm for TCP named A-TCP/RENO is proposed to solve the above problem which requires that the destination should not send ACK for duplicate messages. Through simulation, we note as the speed of the nodes in the network increases, the throughput of TCP/Reno with Epidemic Routing improves slightly over that with DSR. Since there are fewer redundant ACKs in the network and congestion control does not occur unnecessarily, hence improved performance.

Niels Moller, ET. Al. [3] has studied the effect of introducing TCP Westwood+ on regular TCP New Reno by means of analytical modeling and ns-2 simulations. In this author demonstrate that two protocols get different shares of the available bandwidth in the network. With this our result is that the bandwidth sharing between the two protocols depends on one crucial parameter i.e. the ratio between the bottleneck router buffer size and the bandwidth delay product. If the ratio is smaller than one then TCP Westwood+ takes more bandwidth. On the contrary, if the ratio is greater than one, it is TCP New Reno which gets the larger part. Thus studied analytically and by the means of ns-2 simulations, the inter-protocol fairness between TCP Westwood+ and TCP New Reno. With the introduction of TCP Westwood allows solving the well known problem of network under utilization by regular TCP when buffer sizes in routers are set to small values but with gain in the utilization comes at the expense of regular TCP which loses some of its throughput. TCP Westwood+ solves the unfairness problem for large buffer sizes but unfairness problem is still open for small buffers.

O.Ait-Hellal, ET. Al. [4] purpose is to analyze and compare the different congestion and avoidance mechanisms which have been proposed for TCP protocol namely: Reno, New Reno. Reno retains the basic principle such as slow starts and the coarse grain retransmit timer. However it adds some intelligence over it so that lost packets are detected earlier and pipeline is not emptied every time a packet is lost. Reno perform very well over TCP when packet losses are small but when we have multiple packet losses in one window then RENO doesn't perform too well, On the other hand New Reno is a slight modification over TC Reno. It is able to detect multiple packet losses and thus is much more efficient that RENO in the event of multiple packet losses. New-Reno suffers from the fact that it takes one RTT to detect each packet loss. When the ACK for the first retransmitted segment is received segment is received only then can we deduce which other segment was lost. Because of its modified congestion avoidance and slow start algorithm there are fewer retransmits.

Afiqah Azahari, ET. Al. [5] Error control describes how the network handles and detects errors especially in the data link layer present on an overview of error control regarding error detection and error correction. Error control happens in data link layer. We mainly discuss the type of error detection mechanisms that is used to detect the errors and how the errors will be corrected so the receiver can extract the real data. There are different ways to detect error in the data link layer i.e. but not all the methods of error detection can detect error accurately and effectively. Every method has its own specialty, advantage and their own mechanism to detect error. Parity check is simple and can detect all single-bit error. CRC has a very good performance in detecting single-bit error, double errors, an odd number of errors and burst errors while checksum is not efficient as the CRC in error detection when the two words are incremented with the same amount, the two errors cannot be detected because the sum and checksum remain the same.

Bestavros, et al. [6] Author propose a new transport protocol, TCP Boston, that turns the ATM's 53-byte cell-oriented switching architecture into an advantage for TCP/IP. At the core of TCP Boston is the adaptive information dispersal algorithm (AIDA), an efficient encoding technique that allows for dynamic redundancy control. AIDA makes the TCP/IP's performance less sensitive to cell losses, thus ensuring a graceful degradation of the TCP/IP's performance when faced with congested resources. We introduce AIDA and overview the main features of TCP Boston. We present detailed simulation results that show the superiority of our protocol when compared to other adaptations of TCP/IP over ATMs. in online informal organizations. The review consequences of our Facebook application demonstrate that the presumption made by past work that all the connections in informal communities are trusted does not matter to online interpersonal organizations, and it is doable to point of confinement the quantity of assault edges in online informal organizations by relationship rating.

IV. PROBLEM FORMULATION

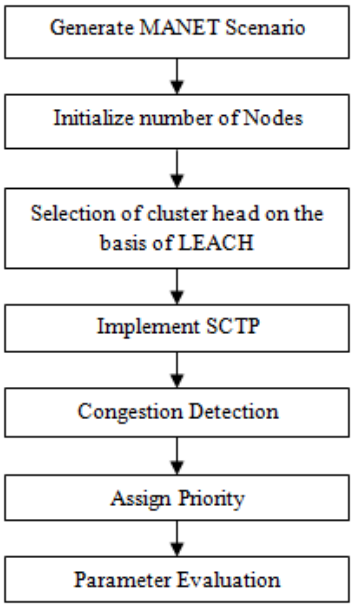
In this network various transmission control protocols have been used for data transmission process. TCP has been used for data transmission communication having different bandwidths and message delays over the network. TCP provides communication using 3-way handshake which sends RTS and ACK comes from 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 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. To overcome this problem SCTP transmission control protocol has been used for the system performance of the system. SCTP provides 4-way 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.

V. PROPOSED WORK

In proposed work some steps to be taken. In first step MANET scenario will be generated with the help of network simulator NS2. Then number of nodes will be initialized through which communication is done and number of nodes

here acting like a mobile devices. As MANET contains mobile devices so node mobility will be done. Then Leach protocol is used to create and maintain clusters & select head cluster on basis of Leach protocol. SCTP has been used for data transmission over wireless network. Sequence of messages has been transmitted over the network. In our work we define the queue & set the queue length & then assign priority for congestion detection & correction and then we evaluate parameters.

Flow of work



VI. RESULTS AND DISCUSSIONS

Network Environment:

Table 6.1

Network Parameters	**Parameters values**
Packet Size	256-2000kb
MAC Type	Mac/802_11
Radio-Propagation Model	Two Ray Ground
Network Interface type	Wireless
Number of Nodes	51
Interface Queue Type	Queue/Drop Trail
Nodes Initial Position	Random
Max Packet in IFQ	2000

We are using NS-2 (Network Simulator 2) and define the simulation area is X dimension of topography is 881, Y dimension of topography is 652, total simulation time is 150s.

- Results

According to our approach we have compared TCP & SCTP over MANET using NS-2 (Network Simulator 2). SCTP reduces congestion problem and provides proper throughput of the system and we got various types of parameters like; throughput, packet delivery ratio, packet loss, end to end delay & energy. Our proposed system achieves higher packet delivery ratio, throughput & energy and achieves less packet loss and delay than existing system & finally we have provided the better results.

- Delay

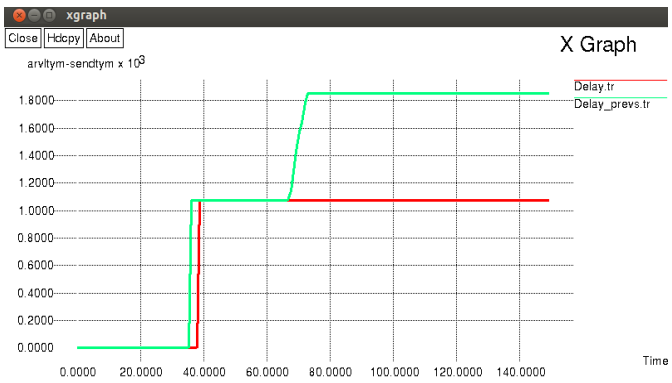


Fig 6.1: Delay

This includes all possible delays caused by buffering during route discovery, latency, and retransmission by intermediate nodes, processing delay and propagation delay. It is calculated as

$$D = (T_r - T_s)$$

Where, T_r is receive time and T_s is sent time of the packet.

- Energy

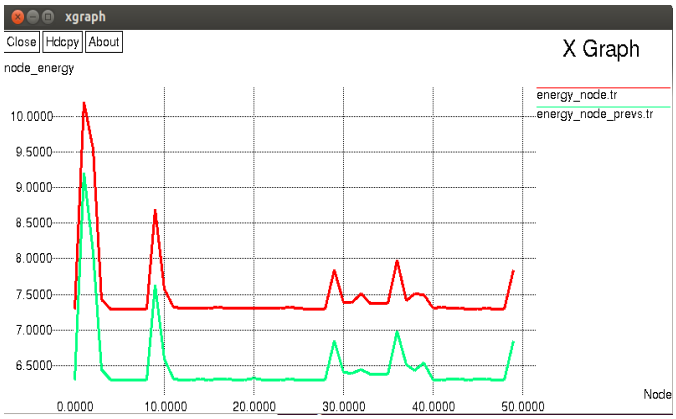


Fig 6.2: Energy

This Graph is use to represent the Energy use to transmit the message from one node to other node. Energy is a property of objects which can be transferred to other objects or converted into different forms, but cannot be created or destroyed. The "ability of a system to perform work" is a common description, but it is difficult to give one single comprehensive definition of energy because of its many forms.

- Packet Loss

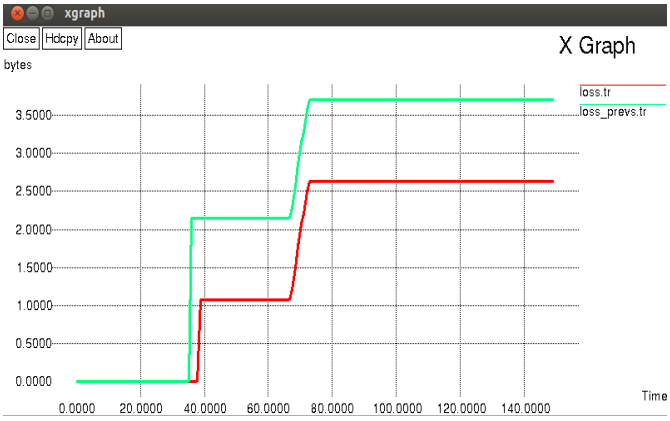


Fig 6.3: Packet Loss

Packet Loss = (total drop packets /total sent packets)

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent.

- Packet Delivery Ratio

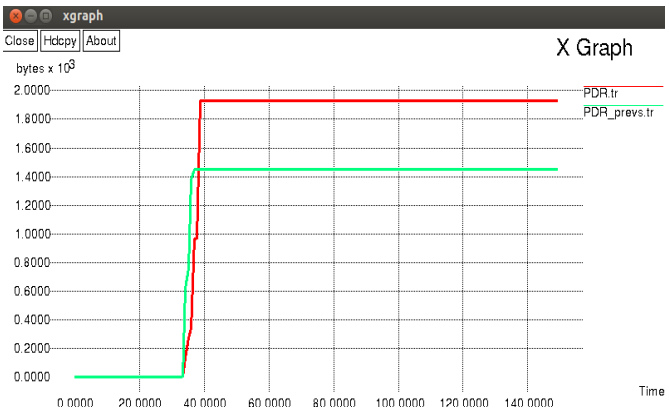


Fig 6.4: Packet Delivery Ratio

It is the ratio of all the received data packets at the destination to the number of data packets sent by all the sources. It is calculated by dividing the number of packet received by destination through the no. of packet originated from the source.

$$PDR = (P_r / P_s) * 100$$

Where, P_r is total packet received and P_s is total packet sent.

- Throughput

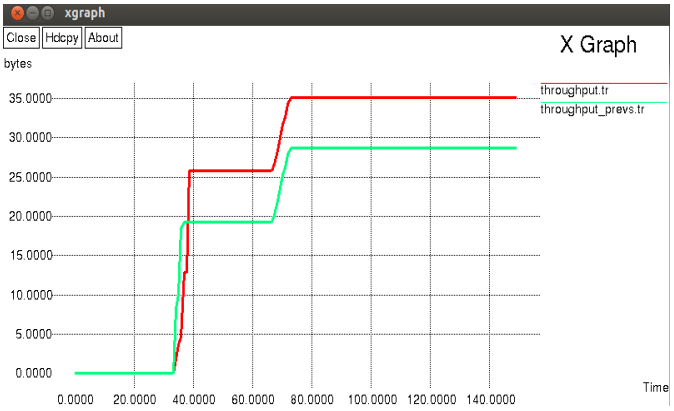


Fig 6.5: Throughput

It is the average at which data packet is delivered successfully from one node to another over a communication network. It is usually measured in bits per second.

Throughput = (no of delivered packets * packet size) / total duration of simulation.

VII. CONCLUSION AND FUTURE SCOPE

In this paper we have compared between TCP and SCTP protocols over MANET. TCP provides communication using 3-way 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 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. To overcome this problem SCTP transmission control protocol has been used for the system performance of the system. SCTP provides 4-way 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. We got various types of parameters & on the basis of these parameters we conclude that our system gives us better results. In the future reference congestion can be avoided by using the congestion controlled approach. The network performance can be enhanced by using the security approach with SCTP protocol. Use of encryption scheme can be done for prevention of data leakage.

REFERENCES

[1] 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.

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

[3] Niels Mollar, "Inter-Protocol fairness between TCP New Reno and TCP Westwood", Route des Lucioles, 2004.

[4] O.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.

.

