www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12462-12464

A Review On Comparative Analysis Of Different Transport Layer Protocols In MANETs

Er. Amritpal Kaur, Er.Pooja Rani
Mtech Research Scholar
Department of CSE RBIEBT
Kharar,India
Email: bhullar_amy21@yahoo.com
Associate Professor
Department of CSE RBIEBT
Kharar,India
Email: poojashrm27@gmail.com

Abstract- *Mobile Ad-hoc Networks (MANETs) allow wireless nodes to form a network without requiring a fixed framework. Ad hoc network is a network which comprises of nodes that use a wireless interface to send information from source to destination. Since the nodes in a network of this kind can serve as routers and hosts so they can forward packets on part of other nodes and run user applications. The traffic scenario basically defines the reliability and capability of information transmission, which creates its performance analysis.TCP (Transmission Control Protocol), is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. Stream Control Transmission Protocol (SCTP) is a transport layer protocol which serve same role to the famous protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).*
In this paper our purpose is to compare different transport layer protocols.

Keywords: SCTP, TCP, UDP, MANET.

1. INTRODUCTION

1.1 MANET

A mobile ad hoc network (MANET) is a continuously self-configuring, network of mobile devices which is without infrastructure and connected without wires. *Ad hoc* is Latin and means "for this purpose". In a MANET each device is open to go without dependence in any direction, and can change its links to other devices immediately. The main challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. These networks may operate by own or may be connected to the internet which is larger. They may contain either one or multiple and variety of transceivers between the nodes. This results in independent, very active topology. MANETs are fairly Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a self-forming, self-healing, peer-peer network in contrast to a mesh network has a central controller. Multi-hop relays date back to at least 500 BC.

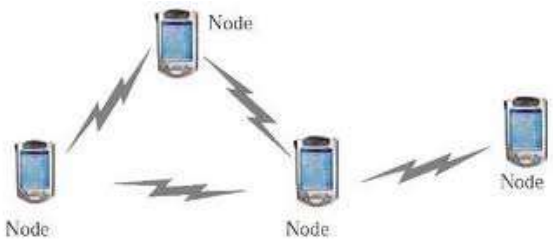

Fig1.1: Mobile Ad hoc Network

1.2 Types of MANET

- Internet based mobile ad hoc networks (I MANETs) are ad hoc networks that link the mobile nodes. Fixed Internet-gateway nodes. For example, multiple sub-MANETs may be linked 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.
- Vehicular Ad hoc Networks (VANETs) are used also in communication. Communication among vehicles and between vehicles and wayside tools. Intellectual vehicular ad hoc networks (In VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners

during collisions of vehicles, during accidents, drunken persons who are driving with phone calls.

- Military MANETs are used by military units which laid on range, integration and security with systems which already exists.

1.3 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 interchange data. TCP is clarified by the Internet Engineering Task Force (IETF) in the Request for Comment (RFC) standards.TCP is a connection-oriented protocol, which is known as connection is recognized and maintained until the application programs at each end have finished interchanging of messages. TCP which works with the Internet Protocol (IP) defines how computers send packets of data to each other.TCP and IP are the basic regulations that define the Internet. It determines how to split application data into packets that networks can send packets to and also accepts packets from the network layer, also manages flow control as it is meant to provide error-free data transmission handles retransmission of dropped or garbled packets as well as acknowledgement of all packets which arrive. In the Open Systems Interconnection (OSI) model which communicates, TCP cover parts of Layer 4, the Transport Layer, and parts of Layer 5, the Layer.

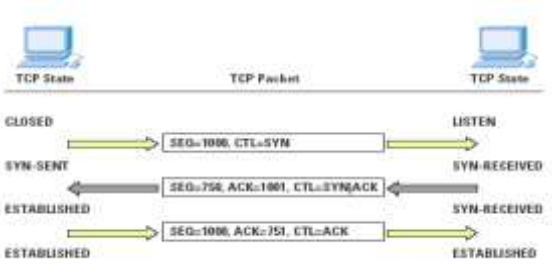

Fig 1.2: TCP protocol

1.4 TCP RENO

To avoid congestion collapse, TCP uses a multi-faceted strategy of congestion-control.TCP maintains a congestion window, in which the total number of difficult packets gets limited for each connection that may be in end-to-end transits. This is somewhat similar to TCP's sliding window used for flow control. TCP uses a scheme called slow start so to increase the congestion window after a connection is initialized and after a break. It starts with a window of two times the maximum segment size (MSS).

Although the beginning rate is short, the rate of increase is very fast, the congestion window increases by 1 MSS so that the congestion window effectively doubles for every round-trip time (RTT). When the congestion window exceeds a threshold the algorithm enters a new state,

called congestion avoidance. In some implementations the early thresh is huge and so the first slow start typically ends after a loss. However, thresh is restructured at the end of each slow start, and will frequently influence subsequent slow starts triggered by time break.

1.5 SCTP (Stream Control Transmission Protocol)

Stream Control Transmission Protocol (SCTP) is a transport layer protocol which serves in a related role to the famous 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 consistent, in order transport of messages with congestion control similar to TCP.

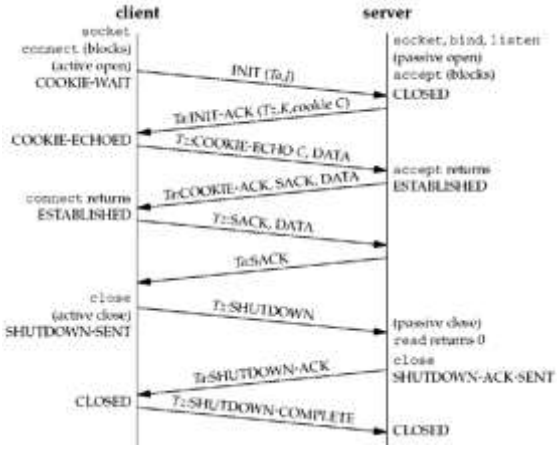

Fig 1.3: SCTP protocol

1.6 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.
- Release of chunks within autonomous streams eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.
- Data transmission is selected by path selection and monitoring the path and test the connectivity of the transmission path.
- Recognition and validation mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks.
- Error detection which is better suitable for Ethernet jumbo frames.

2. LITERATURE SURVEY

Maninder Kaur, Parminder Singh [1] describes that performance of the TCP (Transmission Control Protocol) has been promising incase 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 deal with 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 that are flowing in both directions. The most well known TCP-aware link layer recovery scheme is the Snoop Protocol. It maintains a collection of the packets and whenever a packet loss is detected, it does a local recovery and drops all duplicate acknowledgements.

Narender Sharma et. al [2] According to this paper TCP is the most admired connection oriented transport layer protocol used in the existing internet. Whenever TCP technique applied over MANET, TCP set up new challenges in respect of network congestion and non-congestion. Author concentrates to conquer non-congestion losses in the network. There are many researches to differentiate between congestion and non-congestion losses. In this paper author apply various performance parameters for identifying and overcome non-congestion losses of TCP in MANET and their special effects on the network. In accretion to that author rigorous on the non-congestion control mechanism of the TCP scheme in the MANET, and their adoptable solutions. Author put into practice the proposed idea using NS-3 simulator and simulates the communication and the performance of MANET in different scenarios.

Niels Moller, ET. Al. [3] has studied the outcome of introducing TCP Westwood+ on regular TCP New Reno by means of analytical modeling and ns-2 simulations. In this author reveal that two protocols get different shares of the available bandwidth in the network. With this our effect is that the bandwidth sharing between the two protocols depends on one decisive parameter i.e. the ratio between the bottleneck router buffer size and the bandwidth wait product.TCP Westwood+ takes extra bandwidth when ratio is smaller than one. On the converse, TCP New Reno gets the larger part if ratio is greater than one. Thus after studing analytically and by the means of ns-2 simulations, the inter-protocol equality between TCP Westwood+ and TCP New Reno. With the beginning 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. The lost packets are detected earlier and pipeline is not emptied every time a packet is lost as it adds some intelligence over it. Reno perform very well over TCP when packet losses are tiny but when we have plentiful packet losses in one window then RENO doesn't carry out too well. On the other hand New Reno is a slight alteration 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. The other segment which was lost can be deduced when the ACK for first retransmitted segment is received. For the reason that its modified congestion avoidance and slow start algorithm there are fewer retransmits.

Shiying Lei, ET. al. [5] It describes about the ICWN i.e. Intermittently Connected Wireless Networks especially when Epidemic Routing is used to appraise the act or Delay/disruption Tolerant Networks (DTN), have concerned attention from researchers because of their intrinsic characteristics including extended latency, short data rate and irregular connectivity. It also shows that the Epidemic Routing in ICWN degrades the performance of TCP because multi-copy data packets cause copied ACK's , and in turn reduce the transmitting rate of TCP. Then an better algorithm for TCP named A-TCP/RENO is planned to resolve the above problem which requires that the destination should not send ACK for replicated messages. Through the simulation, we note down as the speed of the nodes in the network increases, the throughput of TCP/Reno with Epidemic Routing improves slightly over that with DSR performance can be improved as there are fewer redundant ACKs in the network and congestion control does not occur unreasonably.

Bestavros et al. [6] Author proposes a new transport protocol, TCP Boston that turn the ATM's 53-byte cell-oriented switching structural design into an advantage for TCP/IP. At the center of TCP Boston is the adaptive knowledge dispersal algorithm (AIDA), an efficient encoding method that allows for dynamic redundancy control. AIDA makes the TCP/IP's presentation less sensitive to cell losses, thus ensuring a refined filth of the TCP/IP's performance when faced with overcrowded resources. We initiate AIDA and overview the main features of TCP Boston. We nearby the detailed simulation consequences that show the advantage of our protocol when compared to other adaptations of TCP/IP over ATMs.

Afiqah Azahari, ET. Al. [7] Error control describes how the network is handled and it detects errors especially in the data link layer which is present on an idea of error control regarding error detection and error correction. We mainly talk about the type of error detection mechanisms that is used to notice the errors and how the errors will be corrected so the receiver can take out the actual data. There are diverse ways to detect error in the data link layer i.e. but not all the method of error detection can detect error precisely and successfully. Every method has its own area of expertise, advantage and their own apparatus to detect error. Parity check is straightforward and can notice all single-bit error. CRC has a very good concert in detecting single-bit error, double errors, an odd number of errors and burst errors while checksum is not resourceful as the CRC in error detection when the two words are incremented with the same quantity, the two errors cannot be detected because the sum and checksum stay the identical.

3. APPROACHES 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 interchange the data. TCP is clarified by the Internet Engineering Task Force (IETF) in the Request for Comment (RFC) standards.TCP is a connection-oriented protocol, which is known as connection is recognized and maintained until the application programs at each end have finished interchanging of messages. TCP which works with the Internet Protocol (IP) defines how computers send packets of data to each other.TCP and IP are the basic regulations that define the Internet. It determines how to split application data into packets that networks can send packets to and also accepts packets from the network layer, also manages flow control as it is meant to provide error-free data transmission handles retransmission of dropped or garbled packets as well as acknowledgement of all packets which arrive. In the Open Systems Interconnection (OSI) model which communicates, TCP cover parts of Layer 4, the Transport Layer, and part of Layer 5.

SCTP (Stream Control Transmission Protocol)

Stream Control Transmission Protocol (SCTP) is a transport layer protocol which serves in a related role to the famous 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 consistent, in order transport of messages with congestion control similar to TCP. In SCTP, when one or both endpoints of a connection can consist of more than one IP address then Multi-homing is supported, which enables transparent fail-over between superfluous network paths. In SCTP head-of-line blocking is eliminated unnecessary when release of chunks within independent streams, as opposed to TCP byte-stream delivery.

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. It has no handshaking dialogue, and thus depiction any unruliness of the underlying network protocol to the user's program. There is no assurance of release, ordering, or duplicate protection. UDP provides checksums for data consistency, and port numbers for addressing dissimilar functions at the source and destination of the datagram. With UDP, computer applications can drive messages, in this holder referred to as datagram, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. UDP is appropriate for purposes where error checking and correction is not necessary or is performed in the application, avoiding the transparency of such dispensation at the network interface level.

CONCLUSION

Approach Used	Advantages	Disadvantages
TCP	**1**.It determines how to break application data into packets that networks can transport, send packets to and accept packets from the network layer, manage flow control, and as it is meant to give error-free data communication handle retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive. **2.** TCP always guarantees three things - your data reaches its target, it reach there in time and it reaches there without duplication. **3.** In TCP, since all the work is done by the operating system, so you just want to sit back and stare at the show. Even the debugging is in use to care of by your OS. **4**. It automatically breaks up data into packets for you. **5**. It is slower in functioning than UDP	**1.**Since, all the work is being done by OS, as a result if there are bugs in your OS, then you will appearance many troubles like troubles in surfing and downloading contents from the net. **2.**TCP cannot be used for broadcast and multicast connections. **3.**TCP doesnot support multi streaming. **4.**It doesnot support multi homing. **5**.It doesnot support preservation of message boundaries. **6.**In TCP there is unordered message delivery.
SCTP	**1**.It provides some of the same service features of both it is message-oriented like UDP and ensures consistent, consecutively transport of messages with congestion control like TCP	**1.**This is a connection-oriented protocol.

UDP	**1.**UDP provides checksums for data veracity, and port information for addressing different functions at the source and destination of the datagram. Broadcast and multicast connections are available with UDP which is not the case with TCP. **2.** It does not restrict you to connection based communication model **3.** Much faster than TCP	**1**.It has no handshaking dialogues, no guarantee of delivery, ordering, or duplicate protection **2**.There are no guarantee with UDP. It is promising that a packet may not be delivered, or delivered twice, or delivered not in time. **3**. you have to manually break the data into packets

REFRENCES

[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] 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 410-415.

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

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

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

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

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

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

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

[12] Ghazaleh, H "Enhancement of throughput time using MS-TCP transport layer protocol for 4G mobiles", ISSN 978-1-4244-2205-0, pp. 1 – 5, IEEE, 2008.

[13] Boussen, S. "Performance analysis of SCTP protocol in WiFi network" Communications and Networking, 2009. ComNet 2009, ISSN 978-1-4244-5134-0, pp 1-5, IEEE, 2009.

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

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