Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

A Study Comparing the Various TCP Versions Used in Wireless Networks

[1]Sunil Kumar Gujjula, [2]Kanuparthi Priyank, [3]Anusha Kudithikunta, [4]M Jawahar

[1,2,3]Assistant Professor, Department of CSE, Narsimha Reddy Engineering College, Secunderabad, Telangana
[4]Associate Professor, Department of CSE, Narsimha Reddy Engineering College, Secunderabad, Telangana

ABSTRACT: *For the majority of Internet applications, Transmission Control Protocol, or TCP, has been the protocol of choice. TCP enables reliable, organized, and error-checked data transfer between hosts running applications that are communicating with one another across an IP network. TCP versions may function at considerably different levels depending on a variety of factors, including round-trip time (RTT), throughput, latency, and bandwidth variation. In light of the aforementioned factors, we examine how well different TCP versions function.*

Keywords: Round trip time (RTT), error, and control protocol (TCP).

I. INTRODUCTION

Currently, IEEE 802.11 Wireless Local Area Networks (WLANs) employ Transmission Control Protocol (TCP) extensively. Due to its ability to create dependable connections via acknowledgements (ACKs), TCP is widely used in networking communication. The IEEE (802.11 protocols) were created for WLANs by the Institute of Electrical and Electronics Engineers (IEEE). Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is used at the MAC layer of the 802.11 protocols in place of Carrier Sense Multiple Access with Collision Detection (CSMA/CD). All access points (APs) and wireless nodes may equitably share the wireless channels thanks to CSMA/CA.

There are many different versions of TCP that are utilized in modern communication networks, including 802.11 WLANs. Some individuals believe that users should never utilize the same TCP version twice in 802.11 WLANs. In every case, the users must choose the best version. Actually, it is not unchangeable. This study aims to determine if there is always a significant difference between the versions of TCP used in 802.11 WLANs.

The goal of the tests is to determine if the performance varies depending on four parameters. Network Simulator 2 (NS2) software is used to replicate the experiment conditions. The throughputs of TCP nodes in various circumstances are then determined by examining the trace files produced during the testing. It is possible to determine which tcp method is superior based on the aforementioned parameters by examining the differences between Throughputs, Rtt, Delay, and varying Bandwidth. The comparison of various TCP versions in 802.11 WLANs is the subject of this paper as a result.

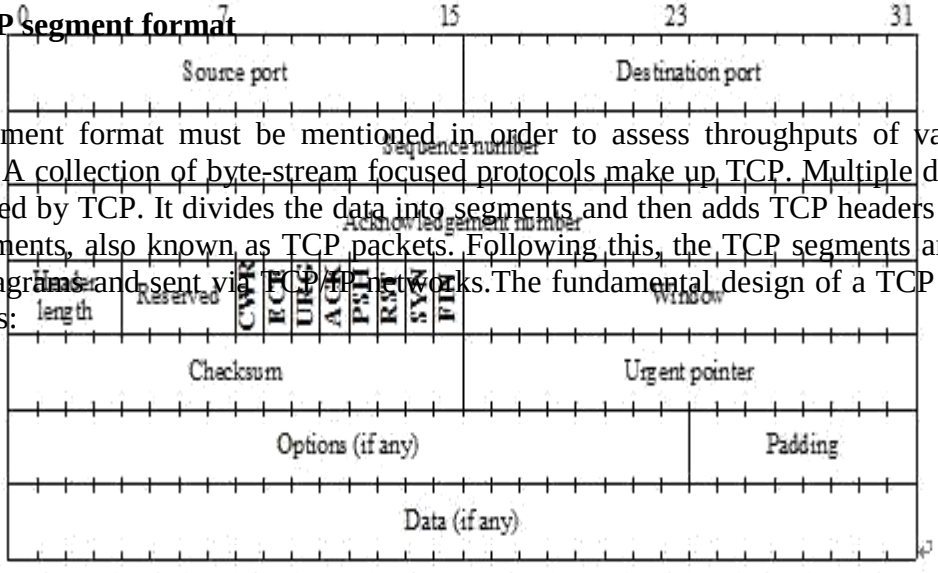
First, certain theoretical background relevant to this thesis must be introduced in this work, such as TCP and 802.11. It also includes an issue statement. The issue described in this section is covered here. The purpose of the third section is to describe the specifics of

simulation scenarios created using NS2. The simulation results are then shown and analyzed in the next section, followed by the conclusion.

1.1 Transmission control protocol

One of the primary protocols making up the TCP/IP protocol suite is TCP. The Internet Protocol (IP) protocol is primarily in charge of handling data packets in the TCP/IP protocol suite, while the TCP protocol is responsible for establishing a connection between two nodes in TCP/IP networks [1]. The Internet Engineering Task Force (IETF) has produced a number of Request for Comments (RFCs) that specify TCP protocols, most notably RFC793 [2].TCP was first created to provide dependable connections for various faraway sites to exchange data consistently across various networks. The scientists soon discovered that due to each network's unique addressing mechanism, maximum packet size, latency, and other factors, it was highly challenging to transfer data in heterogeneous networks error-free. The issues were brought on by dropped, damaged, or duplicate packet deliveries. TCP was created to address the issues by detecting duplicate packets, retransmitting lost packets, and assessing transmission quality by issuing ACKs. The technique for error detection and retransmission ensures that the data connection transmission is maintained. [3]A strong connection is necessary for a successful communication network, and TCP is often employed because of its benefits. A dependable network communication protocol is TCP. Typically, traffic is never created until an effective connection has been established between a sender and a receiver. The connection is full-duplex since it is bi-directional. Both senders and receivers keep an eye on the sessions' progress throughout. The receivers must acknowledge each data packet. Additionally, the senders will retransmit the packets if the receivers notify them that they have not received the packets. TCP is thus used to build trustworthy connections. [3]

1.1.1 TCP segment format



TCP segment format must be mentioned in order to assess throughputs of various TCP versions. A collection of byte-stream focused protocols make up TCP. Multiple data streams are handled by TCP. It divides the data into segments and then adds TCP headers to produce TCP segments, also known as TCP packets. Following this, the TCP segments are wrapped as IP datagrams and sent via TCP/IP networks.The fundamental design of a TCP segment is as follows:

Figure 1.1. TCP segment format [3]

Table 1.1. The fields in a TCP segment [3]

Each field in the TCP segment indicates different functions. The details about each field are listed in Table 1.1:

Control Bits: As mentioned, TCP does not use a separate format for control messages. Instead, certain bits are set to indicate the communication of control information. The six bits are:

Subfield Name	Size (bytes)	Description
URG	1/8 (1 bit)	***Urgent Bit:*** When set to 1, indicates that the priority data transfer feature has been invoked for this segment, and that the *Urgent Pointer* field is valid.
ACK	1/8 (1 bit)	***Acknowledgment Bit:*** When set to 1, indicates that this segment is carrying an acknowledgment, and the value of the *Acknowledgment Number* field is valid and carrying the next sequence expected from the destination of this segment.
PSH	1/8 (1 bit)	***Push Bit:*** The sender of this segment is using the TCP push feature, requesting that the data in this segment be immediately pushed to the application on the receiving device.
RST	1/8 (1 bit)	***Reset Bit:*** The sender has encountered a problem and wants to reset the connection.
SYN	1/8 (1bit)	***Synchronize Bit:*** This segment is a request to synchronize sequence numbers and establish a connection; the *Sequence Number* field contains the initial sequence number (ISN) of the sender of the segment.
FIN	1/8 (1 bit)	***Finish Bit:*** The sender of the segment is requesting that the connection be closed.

1.1.2 Connection establishment

TCP must establish a strong connection in order to send data consistently. Consequently, how does TCP establish a connection between two nodes? TCP establishes a trustworthy connection via a three-way handshake. The following diagram illustrates a three-way handshake:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

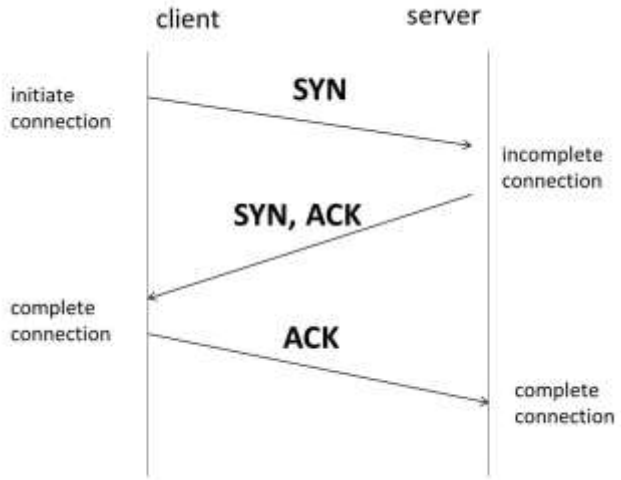


Figure 1.1.2. The progress of the 3-way handshake [5]

The sender delivers a unique TCP segment to the recipient during the first handshake. There isn't any application data in this segment. Only the TCP header containing the SYN is present.

Thus, a SYN segment is one with the bit set to 1. A steady connection may be established by synchronizing the sender and receiver using the SYN segment. The SYN segment is transmitted after being enclosed in an IP packet. The receiver will transmit a connection-granted segment back to the sender after accepting the SYN segment. This section is sometimes referred to as the SYN/ACK segment. There is yet no application data in this area. The initial sequence number (ISN) is ISN (A) +1 in the acknowledgement number field, while the SYN bit is still set to 1 in the connection-granted section. Additionally, the receiver establishes its own initial sequence number ISN (B) and inserts it into the TCP header's sequence number field. The sender will transmit the second segment to the recipient in order for them to acknowledge receiving the SYN/ACK segment once they have accepted it. This section, which is also referred to as the "ACK segment," is used to inform the receiver that it is okay for them to establish a connection. when then, the sender will transmit the data when the connection has been established. The SYN bit is changed from 1 to 0 at the same moment since the connection has been established. [6]

1.2. 802.11

IEEE created the 802.11 family of telecommunications standards to deploy WLANs. Wireless communication has been more popular since World War II, but there were no overarching rules to govern its protocol management. Thus, the first 802.11 protocol for wireless local area networks was published by IEEE in 1997. The original 802.11 protocol for WLANs is 802.11-1997; however, 802.11b is the first protocol that has gained widespread acceptance. The most widely used 802.11 protocols are 802.11b and 802.11g, which were derived from the original 802.11 standard. Typically, the 2.4 GHz to 5 GHz range is where 802.11 technologies operate. [7]

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

The Table lists some of the most significant 802.11 protocols, but not all of them.

2.3. More details about 802.11 protocols in Table 2.3 can be seen below the table:

- 802.11

The first version of 802.11 is also called 802.11-1997 because it was released in 1997 and clarified in 1999. However, it is replaced by updated 802.11 protocols and is not used any more now. 802.11-1997 operated at 1 Mbps or 2 Mbps. The air interface Modulation scheme that the 802.11-1997 takes is direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). The maximum data rate of 802.11-1997 is 2 Mbit/s. [7]

- 802.11a

802.11a is an extension to the 802.11-1997 and it was released in 1999. Many versions of 802.11 work in 2.4 GHz band, which makes channels be crowded. As an improved version of original 802.11, the work frequency band for 802.11a is 5 GHz which improves the quality of wireless communication obviously. Nevertheless, high work frequency band also brings 802.11a a disadvantage: the effective cover range of 802.11a is less than other 802.11 protocols working on 2.4GHz frequency. The physical layer modulation method of 802.11a is orthogonal frequency division multiplexing (OFDM) rather than DSSS or FHSS. The maximum data rate of 802.11a is 54 Mbit/s. [7]

Table 1.2 Some major 802.11 protocols [7]

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

- 802.11b

802.11b was released in 1999 and it was improved directly from the original version of 802.11. It operates at the same frequency band with 802.11-1997 which is defined at 2.4 GHz. Since the decrease of the price and dramatic improved throughput, 802.11bwas accepted widely and rapidly by the users. Although the 802.11b improves the quality of network transmission positively, it is still suffering from interferences because many other electronic devices or 802.11 protocols also work at 2.4 GHz, such as some microwave ovens, 802.11g\n, and so on. The physical layer modulation method of 802.11b is DSSS. The maximum data rate of 802.11b is 11 Mbit/s. [7]

- 802.11g

802.11g was released in 2003, and it is a version that combines some specifications from 802.11a and 802.11b. The 802.11g also works at 2.4GHz like the 802.11b while it also uses OFDM in its air interface like the 802.11a. The 802.11g is able to have higher data rate such as 54 Mbit/s. [7]

- 802.11n

802.11n was released in 2009. It develops the 802.11 protocols by adding three

More multiple-input multiple-output (MIMO) antennas, which improves the throughputs compared to old protocols. The maximum bandwidth may be 40 MHz, not 20 MHz like before. Moreover, the maximum data transmission rate is improved to 150 Mbit/s. The air interface modulation scheme is OFDM just like 802.11a. [7]

- 802.11ac

802.11ac might be the latest developing version of 802.11 family. It aims to provide higher throughputs in the 5 GHz frequency band. As an improvement of 802.11n, the 802.11ac has 8 MIMO streams. The maximum bandwidth can reach to 160 MHz and the maximum data rate may be 6.93 Gbit/s. [7]

As shown in Table 2.3, the bandwidth of the latest 802.11 protocol is bigger and the

Data rate of 802.11 protocols is faster and faster. In 1999, a trade association called Wi-Fi Alliance was formed to operate wireless local area network brand named “Wi-Fi”.The 802.11 protocols support the Wi-Fi products. The wireless network products are allowed to use the brand “Wi-Fi” after they are certificated by the Wi-Fi alliance. [8]

The WLAN provides wireless service to hosts so that the users can access the networks like Internet without any cable. By deploying WLANs and applying the 802.11 protocols, people can access the wireless networks seamlessly with any handy electric devices like smartphones, laptops, or tablets while they are travelling in museums, airports, or schools.

1.2.1. 802.11 operation modes

802.11 protocols have two kinds of operating mode: one is infrastructure mode, and the other one is Ad hoc mode. The configuration of the infrastructure mode is shown in Figure 2.3. In the infrastructure mode, the wireless devices access traditional wired networks like Internet through at least one wireless AP. The AP is a base station and is connected to the

wired networks. The APs are responsible for managing data exchange between wireless and wired networks. [9]

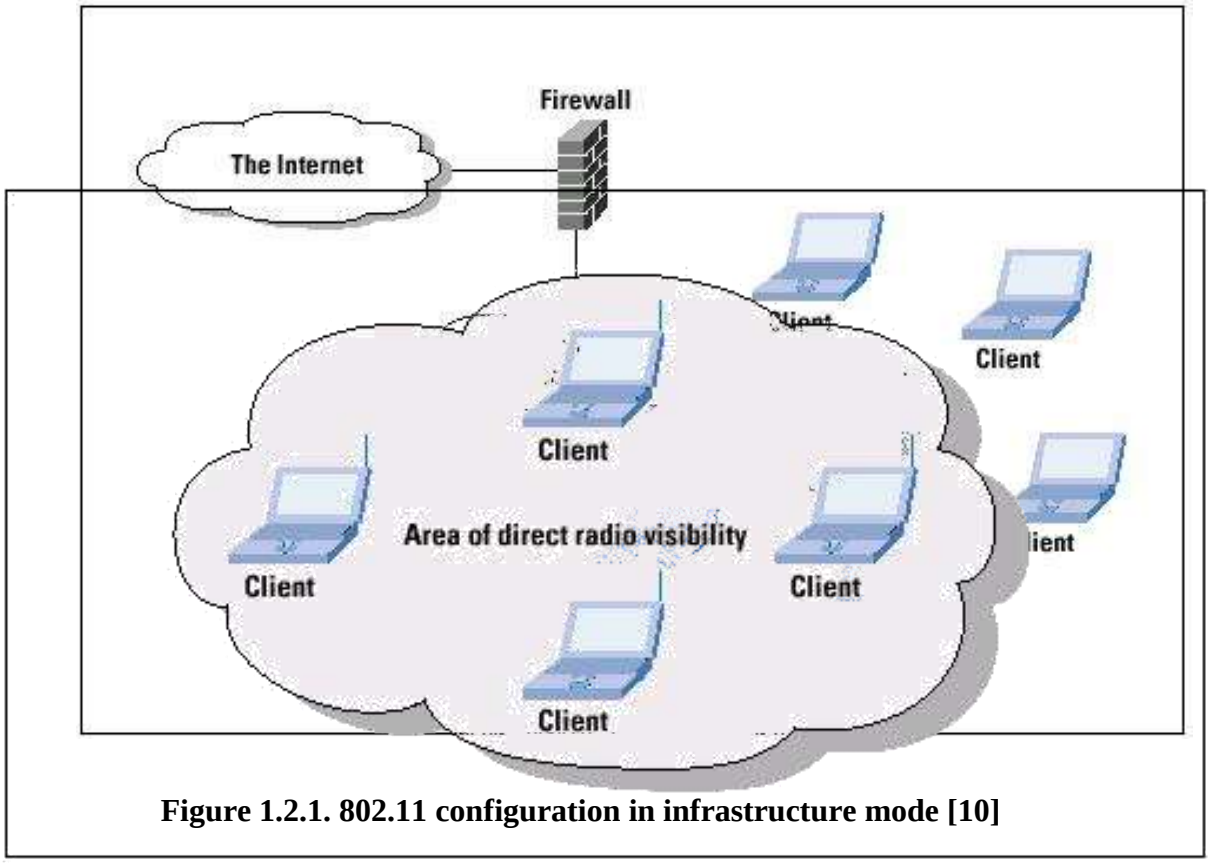


Figure 1.2.1. 802.11 configuration in infrastructure mode [10]

The configuration of the ad hoc mode is shown in Figure 2.4. In the ad hoc mode, the wireless clients communicate with each other directly without any APs or routers. The clients are equal peers which support 802.11 ad hoc mode. The clients in the ad hoc mode forward the data for other peers. The routines are operated by the hosts themselves in the ad hoc mode, and the routing is dynamic depending on the network connectivity. The ad hoc mode makes the WLANs be easy to be deployed and flexible, which is very useful for some specific areas just like military. If a node is broken or destroyed, the network can fix itself by reorganizing the routing dynamically. [8]

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

Figure 1.2.1 a. 802.11 configuration in Ad hoc mode [10]

In this paper, how an artificial bottleneck channel affecting the throughputs of different versions of TCP is researched. So, a set of wired-cum-wireless networks with base stations are designed. Due to every scenario having a base station, only the infrastructure mode is discussed here.

1.2.2. 802.11 MAC

802.11 protocols specify media access control (MAC) and physical (PHY) layers of the OSI model. 802.11 protocols use CSMA/CA as a method in MAC layer instead of CSMA/CD to access the wireless channels [11]. Currently, most of 802.11 protocols use Distributed Coordination Function (DCF) scheme in CSMA/CA. In CSMA/CA with DCF, wireless nodes listen to the channel firstly for a Distributed Inter Frame Space (DIFS) interval when they want to send data packets. Then, if the channel is free, they will send the packets. If the packets are received, the receivers will send acknowledgment (ACK) frames after a Short Inter Frame Space (SIFS) interval. If the senders do not receive ACKs, the senders will think collisions have occurred during transmission.

Once any sender confirms last packet is lost, it will send the same packet again when the channel is idle after another DIFS interval. [12] If the channel is still not free at the beginning, the node will wait for another random period of time until the channel is idle. In the infrastructure mode, CSMA/CA with DCF enables all wireless nodes including the APs to share the wireless channels fairly. By CSMA/CA, the wireless nodes including base stations have the same priority to send their data packets in shared channels, which is quite important in this paper. [13]

1.3. Adhoc On-demand Distance Vector Protocol (AODV)

The mobile Adhoc networks are the finest candidates for the AODV algorithm. Both unicast and multicast routing are both possible with it. Being an on-demand algorithm, it only constructs the various routes between nodes when source nodes request them. As long as the sources need them, it keeps up these pathways. Additionally, AODV creates trees that link the individuals in a multicast group. The group members and the nodes required to link them are made up of the trees. To guarantee the routes are current, AODV employs sequence numbers. It has no loops, starts on its own, and grows to many mobile nodes. A route request is used by AODV to generate routes.

Cycle of / route respond queries. A route request (RREQ) packet is broadcast throughout the network whenever a source node needs a route to a destination for which it does not already have one. As they build up backwards references to the source node in the route tables, nodes receiving this packet update their information for the source node. The RREQ includes the

most recent sequence number for the destination that the source node is aware of in addition to the source node's IP address, current sequence number, and broadcast ID. If a node receiving the RREQ is either the destination or has a route to the destination with a corresponding sequence number higher than or equal to that in the RREQ, it may send a route reply (RREP). It unicasts an RREP back to the source if such is the case. In all other cases, it repeats the RREQ. Nodes record the source IP address and broadcast ID of the RREQ. They trash the RREQ and do not transmit it if they receive an RREQ that they have previously processed.

Nodes create forward references to the destination as the RREP spreads back to the source. The source node may start forwarding data packets to the destination as soon as it gets the RREP. The source may update its routing information for that destination and start utilizing the better route if it subsequently gets an RREP with a higher sequence number or one with the same sequence number but fewer hops. The path will continue to be maintained so long as it is used. As long as data packets are routinely moving from the source to the destination via a given path, the route is deemed active. The connections will time out and finally disappear from the intermediate node routing tables once the source stops transmitting data packets. The source node is informed of the now-impossible destinations via a route error (RERR) message sent by the node upstream of the break if a link break occurs while the route is active. If the source node still wants to find the route after getting the RERR, it may restart the route discovery process.

Similar configurations are used for multicast routes. When a node wants to join a multicast group, it broadcasts an RREQ with the multicast group's IP address as the destination and the 'J' (join) flag set to signal that it wants to join. Any multicast tree node that has received this RREQ and has a recent enough sequence number for the multicast group may issue an RREP. The nodes transmitting the message create pointers in their multicast route tables as the RREPs spread back to the source. The source node maintains track of the path with the most recent sequence number as it gets RREPs, and after that, the shortest hop count to the next multicast group member. The source nodes will unicast a Multicast Activation (MACT) message to its chosen next hop after the designated discovery time. The objective of this message is to activate the route.

A node that put up a multicast route pointer but does not receive this message will time out and destroy the reference. It will also have been keeping track of the optimal route from the RREPs it got if the node receiving the MACT was not already a member of the multicast tree. Therefore, it must also unicast a MACT to its subsequent hop, and so on, until it reaches a node that was formerly a part of the multicast tree. For as long as a route is in use, AODV maintains it. For the duration of the multicast group, this also entails maintaining a multicast tree. Due to the mobility of the network nodes, it is expected that several connection failures will take place along a route throughout its lifespan.

1.4 Priority Queue

In computer networks, when a host sent data packets to the network these packets are stored in a queue and wait for processing by the operating system. The operating system will decide to process which data packet from the queue. At present, the available queues are Drop-Tail Queue, RED (Random Early Detection) Queue, Class Based Queue (includes round robin, priority queue), Fair Queue and Stochastic Fair Queuing.

Mostly used queue type in wireless network is Priority Queue. Working mechanism of Priority Queue is similar to that of Drop-Tail Queue. Drop-Tail follows FIFO order where the packets are entered into the queue at the head and leaves at the tail. But, Priority Queue enqueues the high priority packets at the head and low priority packets at the tail of the queue. By default, in NS-2 routing packets have higher priority whose packets types are PT_TORA, PT_DSR, PT_AOMDV, PT_AODV and PT_MDART.

1.5 Real Time Applications

1.5.1 MPEG-4

Moving Picture Experts Group – MPEG, is a standard codec used to compress voice and video data in digital format and transmits across the digital network. It provides the excellent codec tools for the compression of multimedia such as audio, video and graphics. MPEG-4 provides “object based compression” technique to encode the multimedia scenes. This technique encodes the voice and visual objects independently. An MPEG-4 scene consists of more than one Audio-Video Objects (AVO). Each Video Object (VO) can be encoded in single or multi-layer form. A layer is composed of a sequence of a Group of Video-Object-Plane (GOV). Similar to MPEG-2 frames, VOP supports intra coded (I-VOP), temporally predicted (P-VOP), and bi-directionally predicted (B-VOP) frames. MPEG-4 was mainly aimed at low bit rate (less than 1.5 MBits/sec) video transmissions. .mpg, .dat are the extensions of video files of MPEG. Audio files have .mp1, .mp2, .mp3 extensions.

MPEG-4 provides following functions.

- ✓ MPEG-4 can encode the mixed multimedia data such as speech, audio and video.
- ✓ It has enhanced coding effectiveness over MPEG-2.
- ✓ It is fault tolerant to provide robust communication.
- ✓ It interacts with the audio and video scene generated at the receiver.

Latest MPEG-4 video codec is AVC – Advanced Video Codec. It standardized as ITU H.264. AVC codec offering a compression rate half than that of MPEG-2 with same quality, this represents that it has improvement in video coding. This codec is also used in broadcasting the video to mobile handsets using DMB and DVB-H specified in HD-DVD and Blu-ray high definition optical disc standards.

MPEG-4 Related Standards

a) MPEG-1

MPEG-1 is used in interactive media and video on demand systems. It enables video compression and storage on optical disk, also made available in video CD format. MPEG-1 audio has two coding techniques, one Layer 2 coding used in DBA digital standard, other Layer 3 coding available in MP3 format.

b) MPEG-2

MPEG-2 is audio and video standard used in media applications. It enables digital TV and DVD's with numerous of MPEG-2 decoders are deployed in satellite, set-top boxes and PC's. MPEG-2 video codec is more CPU intensive than MPEG-1.

c) MPEG-4

MPEG-4 is an extended standard over MPEG-2, it is the successor standard to MPEG-2. MPEG-4 extended its applications to rich multimedia presentation, interactivity and lossy networks. It also has improvement in voice and visual codec over MPEG-2, mainly the AVC, HE-AAC and AAC codec which have enabled number of new services and products.

d) MPEG-7 and MPEG-21

MPEG-7 and MPEG-21 are the additional related standards to extend functionality of MPEG. MPEG-4 is integrated with MPEG-7 and MPEG-21 to create new content management features. MPEG-4 carries the streams with metadata and descriptions of MPEG-7. MPEG-21's specifications are being written to complement MPEG-4's content representation.

MPEG-4 Features

1) **Interoperability:** MPEG-4 standard is designed to fit all platforms not only to a specific platform

2) **Scalability:** MPEG-4 provides flexibility in coding and decoding of bit streams and also the resolution can be optimized.

3) **Profiles:** MPEG-4 standard provides different technology profiles for applications which it uses. So service providers use only the subset that suits their applications.

1.6 Motivation

In current communication networks including 802.11 WLANs which support TCP, there are more than one versions of TCP which are being used. Some people think it is always different for users to use different versions of TCP in 802.11 WLANs. The users have

to choose the best version in every scenario. In fact, it is not absolute. The objective of this work is to verify whether there is always big difference to use different versions of TCP in 802.11 WLANs.

The purpose of experiments is to find out whether how the performance is varied based on four factors. The network topology is dumbbell topology in static wireless environment and low mobility environments in wireless network.

1.7 Scope

The scope of the project is

- ✓ Performance evaluation of TCP algorithms in wireless environment by considering the traffic as normal data and multimedia traffic.
- ✓ Metrics considered are throughput, round-trip-time, delay and variation in bandwidth.

1.8 Problem Statement

To evaluate the performance mobility environment by comparing bandwidth. of TCP versions in wireless environment and low the factors rtt, throughput, delay and variation in wireless networks.

1.9 Objectives

The main objective of this report is to identify which tcp version is efficient based on the metrics and understanding the scope for improvement. This project is designed to evaluate four transport protocol versions,

- ✓ Tahoe
- ✓ Vegas
- ✓ Reno
- ✓ Newreno

1.10 Organization of Project

Thesis is organized as follows:

Chapter 2 covers the literature survey; this chapter explains the previous research in TCP versions performance on several factors.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

Chapter 3 covers the hardware and software requirements; this chapter explains hardware components and software components of the project.

Chapter 4 review the implementation, this chapter covers network simulator, performance metrics and topology.

Chapter 5 covers simulation results and analysis.

Chapter 6 covers code of the project.

Chapter 7 covers conclusions of the project

II. Literature Survey

Many works have been done in improving the efficiency of the Transmission Control panels. Work such as congestion control mechanism that controls the sending rate of TCP. Works have been done on the heterogeneous networks with lossy nature like wireless networks for example. Network security and in-depth understanding of TCP/IP stack is another important aspect that is in study in various works. Internet models are introduced to develop the argument to support packet data networking for local and wide area networks that include the internet. The evolution of TCP is a careful balance between innovation and considered constraint. The evolution of TCP must avoid making radical changes that may stress the deployed network into congestion collapse, and also must avoid a congestion control "arms race" among competing protocols.

III.IMPLEMENTATION

3.1 Simulation Environment

Wireless environment

The transport protocols TCP is simulated separately in static wireless network. The topology used is dumbbell topology with five bottleneck links in between the source and destination. The distance between the nodes is 200m, which is the typical communication range of the wireless devices (in ns2 simulator). The position of the wireless nodes is as shown in Fig. 4.1. Two nodes are considered as traffic sources and two nodes are considered as destinations. The network simulator NS-2, version 2.35 is used for simulation. [17]

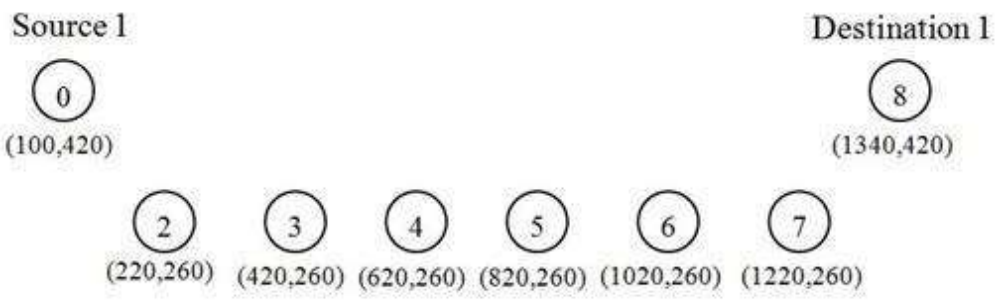


Figure 3.1: Wireless Topology indicating the positions of the nodes.

Table 3.1: Simulation parameters in static wireless environment

Simulation Parameters	
MAC Protocol	IEEE 802.11
Propagation Model	Two-ray Ground
Interface Queue	Priority Queue
Routing Protocol	AODV
Grid size	1500 X 500 m
Distance between the nodes	200 m
Simulation time	100 sec
Transport protocols	TCP, TFRC
Traffic type	MPEG-4

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

Wireless environment

The two transport protocols TCP and TFRC are simulated separately in low mobility environment. Simulation parameters are shown in the following table.

Table 3.2: Simulation parameters in wireless environment

Simulation Parameters	
MAC Protocol	IEEE 802.11
Propagation Model	Two-ray Ground
Interface Queue	Priority Queue
Routing Protocol	AODV
Grid size	1500 X 500 m
Distance between the nodes	200 m
Simulation time	100 sec
Transport protocols	TCP, TFRC
Traffic type	MPEG-4
Low Mobility	Random mobility enabled, no. of nodes 10

3.2 Performance Metrics

The following are the metrics considered.

- ✓ **Throughput:** Throughput is defined as number of bits transmitted per second.
- ✓ **Round-Trip-Time**: **round-trip time** (RTT) is the length of **time** it takes for a signal to be sent plus the length of **time** it takes for an acknowledgement of that signal to be received.
- ✓ **Delay: delay** is the amount of time it takes for the head of the signal to travel from the sender to the receiver.
- ✓ **Bandwidth:** Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time -- usually one second.

V.CONCLUSION

According to observation, TCP Vegas has a high throughput as the number of sources grows.Tcp Tahoe has more received packets at the Receiver side if bandwidth is increased.There is less lag on Tcp Vegas.The TCP Vegas has an extremely short roundtrip time.Tahoe has a high throughput when the bandwidth is increased.Tcp Vegas receives more packets when sources are increased.While the throughput figure varies, the bandwidth, round trip time, and latency are about the same for TCP Reno and TCP New Reno.

VI.FUTURE WORK

TCP's role in supplying a dependable end-to-end data transmission function and implementation of a number of control functions is meant to facilitate effective use of the IP network via a host-based. Many "better-than-TCP" protocol stacks have recently entered the market, most frequently in conjunction with Web server systems. These protocols' performance claims include the ability to work with standard TCP clients and provide download speeds that are faster than those provided by standard TCP protocol implementations. The normal TCP flow control systems, which employ a lower initial RTT estimate to give a more aggressive starting rate, are modified to enable this level of performance. A bigger initial congestion window size or a quicker variation of slow start, in which the transmitting rate is tripled or higher per round-trip time interval, are two further adjustments that might be made.

REFERENCES

[1]https://www.researchgate.net/profile/Srinivasan_Seshan2/publication/3334502_A_comparison_of_mechanisms_for_improving_TCP_performance/links/0fcfd51396b59a5f4c000000/A-comparison-of-mechanisms-for-improving-TCP-performance.pdf

[2] J. Postel, “Transmission Control Protocol”, RFC-793, September 1981.

[3] W. Stevens, “TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms”, RFC-2001, January 1997.

[4] T. Gopinath, A.S.Rathan Kumar, Rinki Sharma,“Performance Evaluation of TCP and UDP over Wireless Ad-hoc Networks with Varying Traffic Loads”, IEEE International Conference
on Communication Systems and Network Technologies, PP: 281-285, 2013, DOI: 10.1109/CSNT.2013.66.

[5] Abdul Razaque Rind, Khurram Shahzad, M.Abdul Qadir, “Evaluation and comparison of

TCP and UDP over Wired-cum-Wireless LAN”, IEEE International Conference on Multitopic Conference, PP: 337-342, 2006, DOI: 10.1109/INMIC.2006.358188

[6] The VINT Project, The Network Simulator – NS-2. [Online].

http://www.isi.edu/nsnam/ns/ns-documentation.html (accessed on 4 Novermber 2011).