Juni Khyat
(UGC Listed Journal)

ISSN: 2278-4632
Vol-9 Issue-1 No.01 January 2019

A Comparative Study of the Different Versions of TCP Used in Wireless Networks

A SANDHYA RANI
Associate Professor
Sandhyarani.alts@gmail.com

K. ANUSHA
Assistant professor
Anushak.alts@gmail.com

PRASANTH KUMAR.M
Assistant Professor
Prasanthkumar.alts@gmail.com

ABSTRACT: *Transmission Control Protocol, or TCP, has been the protocol of choice for most applications on the Internet. TCP ensures the transmission of a stream of data in a reliable, organised, and error-checked fashion between applications executing on hosts that are talking with one another over an IP network. TCP versions may have significantly different levels of performance based on a number of characteristics like round-trip time (RTT), throughput, latency, and variance in bandwidth. In conclusion, we look at the performance of the various TCP versions based on the parameters listed above.*

Keywords:Control protocol,TCP,Error,Round Trip Time(RTT).

I. INTRODUCTION

Currently, Transmission Control Protocol (TCP) is widely used in IEEE 802.11 Wireless Local Area Networks (WLANs). TCP is popular in networking communication because it can provide reliable connections by using acknowledgements (ACKs). 802.11 protocols were developed by Institute of Electrical and Electronics Engineers (IEEE) for WLANs. 802.11 protocols use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in their MAC layer instead of Carrier Sense Multiple Access with Collision Detection (CSMA/CD). CSMA/CA enables all wireless nodes and access points (APs) to fairly share the wireless channels.

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 experiment scenarios are simulated by using the software named Network Simulator 2 (NS2). Then, through puts of TCP nodes in different scenarios are calculated by analyzing trace files generated from the experiments. Through comparing the difference between the Throughputs, Rtt, Delay and varied Bandwidth. it is feasible to find out which tcp algorithm is better based on above factors. That is why the topic of this work is “comparison of different versions of TCP in 802.11 WLANs.

In this work, firstly, some theoretical background related to this thesis needs to be Introduced, such as TCP and 802.11. Secondly, it is problem statement. This part is about the problem discussed in this paper. The third part is to introduce the details of simulation scenarios made by using NS2. Then, the next part is to show and analyze the results of the simulations, and the last part is the conclusion.

1.1 Transmission control protocol

TCP is one of main protocols compositing of TCP/IP protocol suite. In TCP/IP protocol suite, TCP protocol is responsible for building a connection between two nodes in TCP/IP networks whereas Internet Protocol (IP) protocol is mainly responsible for dealing with data packets [1]. TCP protocols are defined in a series of Request for Comments (RFCs) published by the Internet Engineering Task Force (IETF), especially RFC793 [2].In the early days, TCP was developed to provide stable connections for different remote hosts to exchange data reliably in different networks. Soon, the scientists found it was very difficult to transmit the data free of error in heterogeneous networks because each of them has different addressing mode, maximum packet size, delay, and other things. The problems caused that the packets delivered were dropped, damaged, or duplicated. To solve the problems, TCP was designed to detect duplicated packets, check transmission quality by sending ACKs, and retransmit dropped packets. The error detection and retransmission scheme make sure the transmission of data link is maintained. [3]The good communication network needs reliable connection, and TCP is used widely because of its advantages. TCP is considered as a reliable network communication protocol. Usually, an effective connection between a sender and a receiver is always established before the traffic is generated. The connection is bi-directional, which means it is full-duplex. During the sessions, both senders and receivers keep monitoring the state of the sessions. Each data packets must be acknowledged by the receivers. Moreover, if the receivers do not get the packets, they will inform the senders and the senders will retransmit the packets. So, reliable links are established by applying TCP. [3]

1.1.1 TCP segment format

In order to analyze throughputs of different versions of TCP, it is necessary to mention TCP segment format. TCP is composed of a series of byte-stream-oriented protocols. TCP deals with data from multiple data streams. It segments the data, and then adds TCP headers to create TCP segments which are often referred to as TCP packets. After this, the TCP segments are encapsulated into Internet Protocol datagram (IP datagram) delivered in TCP/IP networks.The basic structure of TCP Segment as follows:

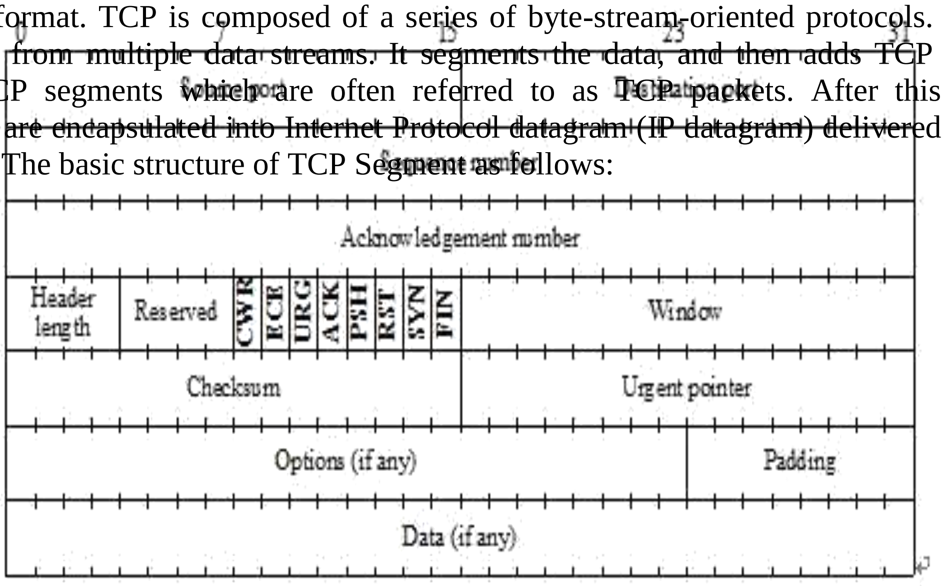
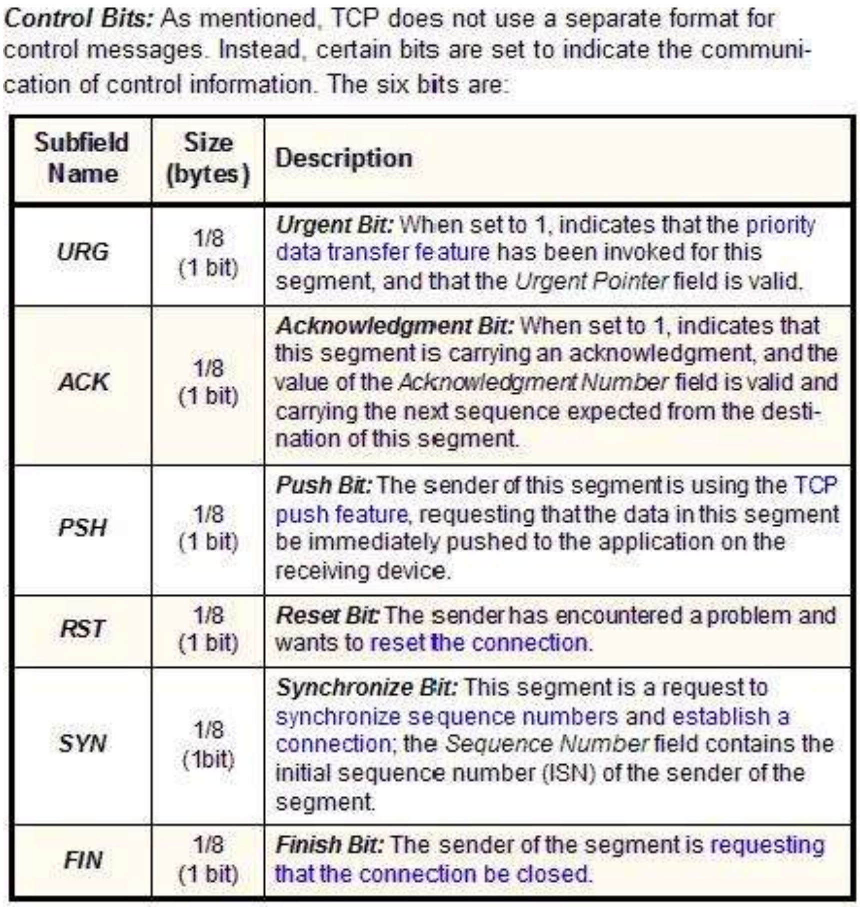


Figure 1.1. TCP segment format [3]

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

For transmitting the data reliably, it is important for TCP to establish a solid connection. So, how does TCP build a connection between two nodes? TCP uses 3-way handshake to establish a reliable connection. The process of a 3-way handshake is shown as follows:

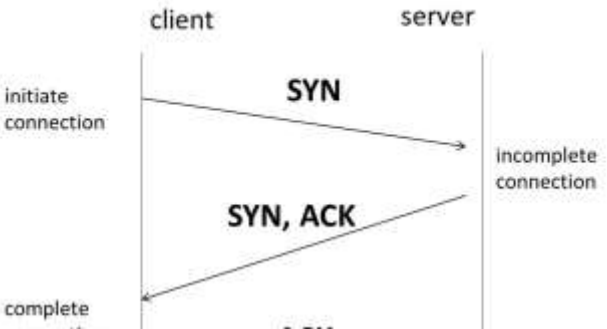


Figure 1.1.2. The progress of the 3-way handshake [5]

In the first handshake, the sender sends a special TCP segment to the receiver. This Segment does not have any application data. It only has the TCP header with the SYN

Bit set to 1, so it is called a SYN segment. The SYN segment is used to synchronize the sender and receiver so that a stable connection can be built. The SYN segment is encapsulated in an IP packet and sent. When the SYN segment is accepted by the receiver, it will send a connection-granted segment back to the sender. So, this segment is also called SYN/ACK segment. This segment does still not contain any application data. In the connection-granted segment, the SYN bit is still set to 1, and the initial sequence number (ISN) is ISN (A) +1 in the acknowledgment number field. The receiver also sets its own initial sequence number ISN (B), and puts it into the sequence number field of the TCP header. After accepting the SYN/ACK segment, the sender will send the second segment to the receiver to acknowledge the SYN/ ACK segment. This segment is to tell the receiver it is fine to establish a connection between them, so this segment may be called ACK segment. Then, the connection is established and the sender will send the data. At the same time, the SYN bit is set to 0 from 1 because the connection has been built. [6]

1.2. 802.11

802.11 is a set of telecommunication standards developed by IEEE to implement WLANs. Since World War II, wireless communication has been used widely more and more but there were no general standards to manage wireless communication protocols. So, in 1997, IEEE released the first 802.11 protocol for wireless local area networks. 802.11-1997 protocol is the original 802.11 protocol serving the WLANs; however, 802.11b is the first widely accepted protocol. Most of 802.11 protocols are developed from the original 802.11, and the most popular ones of them are 802.11b and 802.11g. Usually, the frequency bands where 802.11 protocols work are from 2.4 GHz to 5 GHz. [7]

Some major 802.11 protocols, not all of 802.11 protocols, are shown in the Table

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

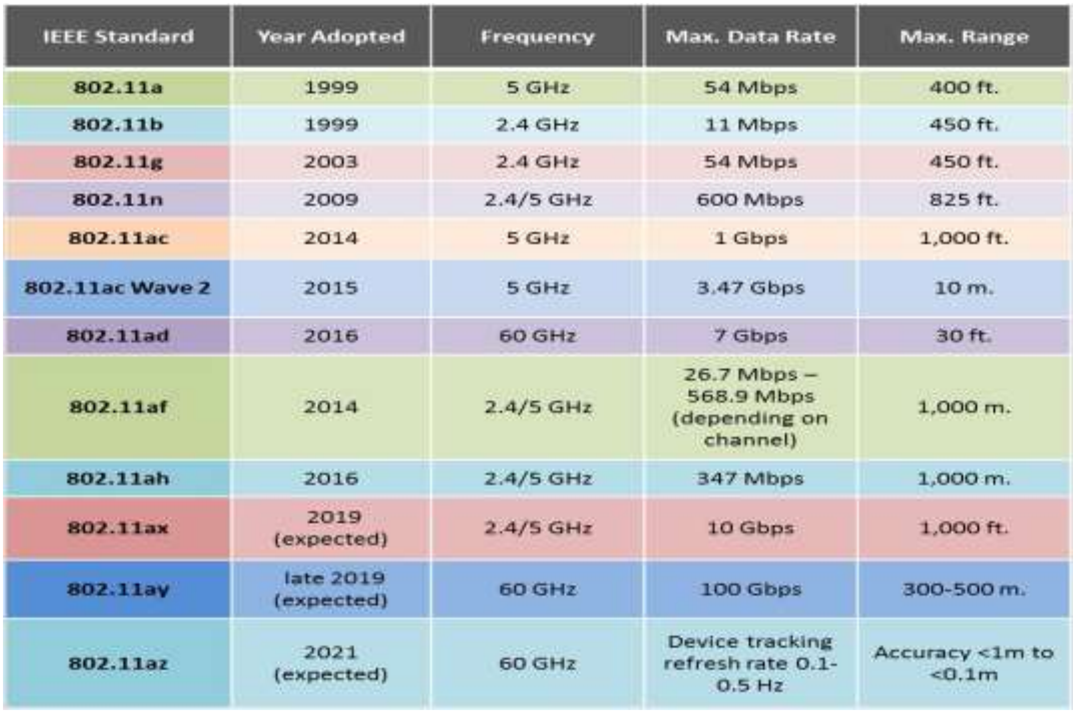
- 802.11

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]

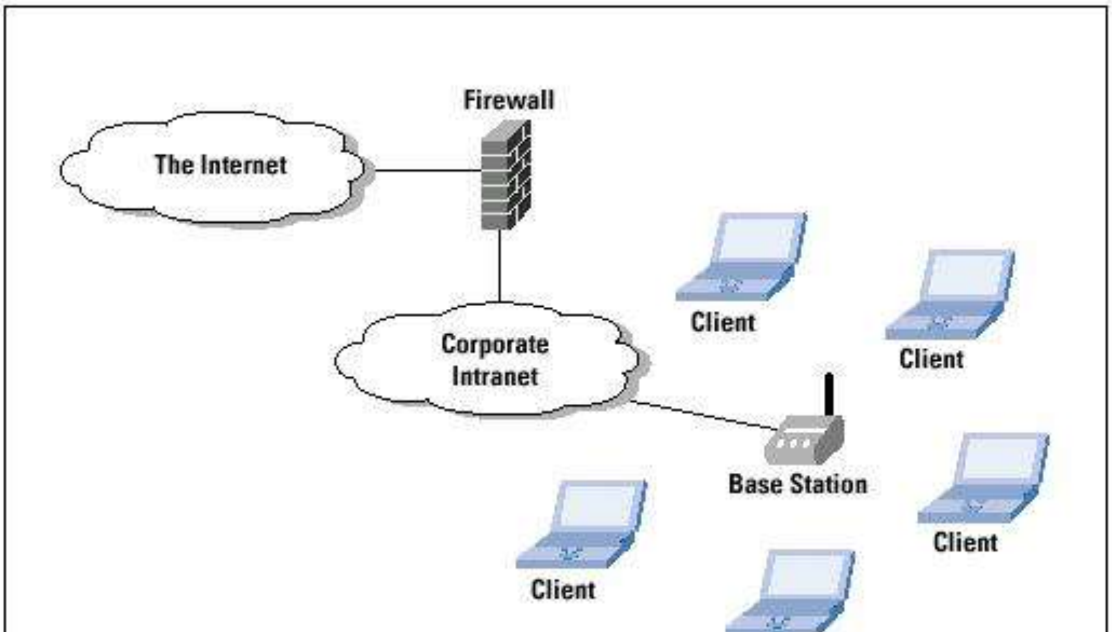


Figure 1.2.1. 802.11 configuration in infrastructure mode [10]

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]

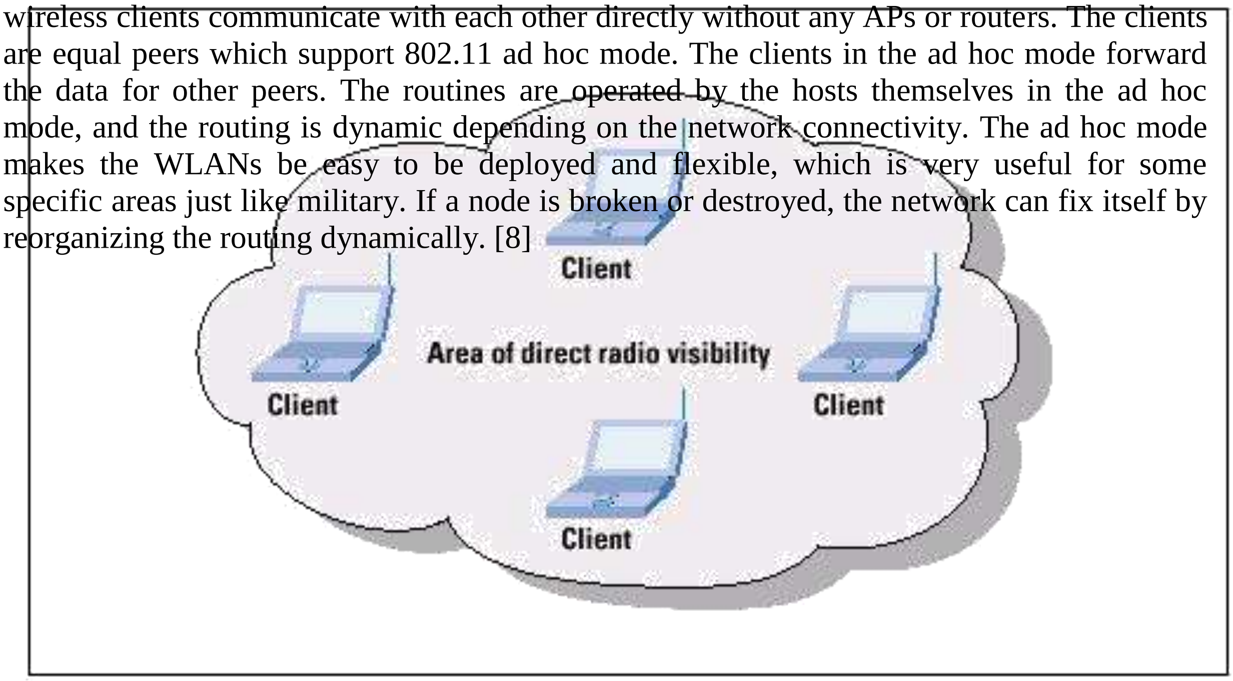


Figure 1.2.1 a. 802.11 configuration in Ad hoc mode [10]

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)

AODV algorithm is best suited for the mobile Adhoc networks. It is capable of unicast routing and multicast routing. It is an on demand algorithm, meaning that it creates the multiple paths between nodes only as desired by source nodes. It maintains these paths as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence number to ensure the freshness of routes. It is loop-free, self-starting, and scales to large number of mobile nodes. AODV builds routes using a route request

/ route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

As the RREP propagate back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

Multicast routes are set up in a similar manner. A node wishing to join a multicast group broadcasts a RREQ with the destination IP address set to that of the multicast group and with the ‘J’ (*join*) flag set to indicate that it would like to join the group. Any node receiving this RREQ that is a member of the multicast tree that has a fresh enough sequence number for the multicast group may send a RREP. As the RREPs propagate back to the source, the nodes forwarding the message set up pointers in their multicast route tables. As the source node receives the RREPs, it keeps track of the route with the freshest sequence number, and beyond that the smallest hop count to the next multicast group member. After the specified discovery period, the source nodes will unicast a Multicast Activation (MACT) message to its selected next hop. This message serves the purpose of activating the route.

A node that does not receive this message that had set up a multicast route pointer will timeout and delete the pointer. If the node receiving the MACT was not already a part of the multicast tree, it will also have been keeping track of the best route from the RREPs it received. Hence it must also unicast a MACT to its next hop, and so on until a node that was previously a member of the multicast tree is reached. AODV maintains routes for as long as the route is active. This includes maintaining a multicast tree for the life of the multicast group. Because the network nodes are mobile, it is likely that many link breakages along a route will occur during the lifetime of that route.

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.

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]

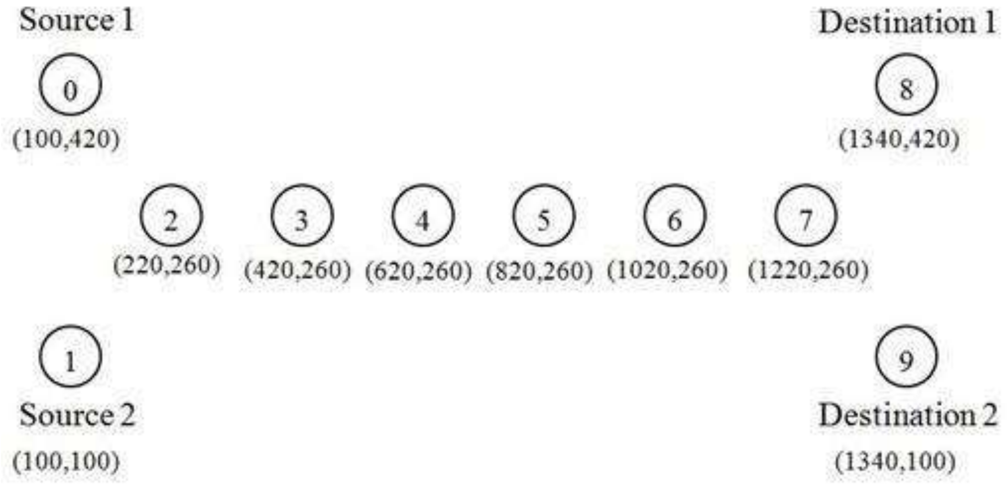


Figure 3.1: Wireless Topology indicating the positions of the nodes.

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

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

- ✓ From observation Tcp Vegas has high throughput if number of sources are increasing.
- ✓ If bandwidth is increased Tcp Tahoe has more received packets at Receiver side.
- ✓ Tcp Vegas has less delay.
- ✓ Round trip time is very less for TCP Vegas.
- ✓ Tahoe has high throughput in case of increasing bandwidth.
- ✓ If sources increased Tcp Vegas has more received packets

- ✓ Bandwidth, round trip time, delay are approximately same for TCP Reno and TCP New Reno, for the value of throughput we can observe a variation.

VI.FUTURE WORK

TCP role in providing a reliable end-to-end data transfer function and incorporation of numerous control functions that are intended to make efficient use of IP network through a host-based. Recently numerous “better-than-TCP” protocol stacks have been appearing in the market, most commonly in conjunction with Web server systems, these protocols performance is claimed that it can interoperate with standard TCP clients, offering superior download performance to a standard TCP protocol implementation. This level of performance is achieved by modifying the standard TCP flow control systems which use a lower initial RTT estimate to provide a more aggressive startup rate. Other modifications may include using a larger initial congestion window size or may use an even faster version of slow start, where the sending rate is tripled, or more, every round-trip time interval.

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 November 2011).