

**Performance Analysis between CSMA/CA and MACA
Protocol**

SUBMITTED BY

Mishuk Kobir Ritu

ID: 101-19-1191

Anamika Saha

ID: 101-19-1194

This Report Presented in Partial Fulfillment of the Requirements for the Degree of
Bachelor of Science in Electronics and Telecommunication Engineering.

SUPERVISED BY

MD. ZAHIRUL ISLAM

Lecturer

Department of ETE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2014

APPROVAL

This Project titled "Performance Analysis between CSMA/CA and MACA Protocol" by Mishuk Kobir Ritu and Anamika Saha have been submitted to the Department of Electronics and Telecommunication Engineering, Daffodil International University in partial fulfillment of the requirement for the Degree of Bachelor of science in Electronics and Telecommunication Engineering. This thesis has been accepted as satisfactory by the honorable members of the Board of examiners after its presentation. The presentation has been held on January 2014.



BOARD OF EXAMINERS

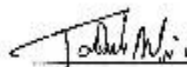
Dr. A.K.M. Fazlul Haque
Associate Professor and Head
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

Chairman



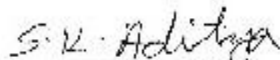
Ms. Shahina Haque
Assistant Professor
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Md. Taslim Arefin
Assistant Professor
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Snbrata Kumar Aditya
Professor
Department of Applied Physics
Electronics and Communication Engineering
University of Dhaka

External Examiner

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty Allah for His divine blessing makes us possible to complete this project successfully.

The special thank goes to our helpful supervisor **Md. Zahirul Islam**, Lecturer, Department of ETE, Daffodil International University, Dhaka. Deep Knowledge & Keen interest of our supervisor in the field of wireless network influenced us to carry out this thesis. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this thesis.

We would like to express our heartiest gratitude to Dr. A. K. M. Fazlul Haque, Associate Professor and Head, Department of ETE, Ms. Shahina Haque, Assistant Professor, Md. Taslim Arefin, Assistant Professor and Dr. Subrata Kumar Aditya, professor, Department of Applied Physics, Electronics and Communication Engineering, University of Dhaka, for their kind help to finish our thesis and also to other faculty members and the staffs of ETE department of Daffodil International University. We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant supports and patients of our parents.

DECLARATION

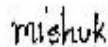
We hereby declare that, this project "Performance Analysis between CSMA/CA and MACA protocol" has been done by us under the supervision of Md. Zahirul Islam, Lecturer, Department of ETE, and Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of B.Sc in Electronics & Telecommunication Engineering degree.

Supervised by:

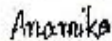


Md. Zahirul Islam
Lecturer
Department of ETE
Daffodil International University

Submitted by:



Mishuk Kubir Rita
ID: 101-19-1191
Department of ETE
Daffodil International University



Anamika Saha
ID: 101-19-1194
Department of ETE
Daffodil International University

ABSTRACT

In a wireless network nodes can be hidden from each other if they are in communication with a central station but not directly with each other. The presence of hidden nodes creates complications for transmitting throughout the network, and also when two or more networks are trying to share the same frequency and physical space. Hidden nodes in a wireless network are out of range of other nodes or a collection of nodes. This kind of problem can be solved in MACA protocol using CTS/RTS handshaking. In this report a comparative analysis based on packet loss and throughput is done between two topologies designed with CSMA and MACA protocol using Network Simulator 2 (NS2).

TABLE OF CONTENTS

CONTENTS	PAGES
Board of Examiners	ii
Acknowledgement	iii
Declaration	iv
Abstract	v
Table of Content	vi-viii
List of Figure	ix
List of Table	x

CHAPTERS

CHAPTER1: INTRODUCTION	1-3
1.1 General Introduction	1
1.2 Goal of the research work	2
1.3 Organizations of the thesis	2
CHAPTER 2: CSMA/CA	4-20
2.1 Overview of CSMA/CA	4
2.2 What is CSMA/CA?	5
2.2(a) Binary Exponential Back-off Algorithm	6
2.3 Flowchart of CSMA/CA	7
2.3(a) Frame Exchange Time Line	8
2.3(b) Network Allocation Vector (NAV)	9
2.4 CSMA/CA Protocol	10
2.5 Usage of CSMA/CA	12
2.6 CSMA/CA uses Wireless LAN	12
2.7 Why uses WLAN in CSMA/CA?	13
2.8 What is Hidden Node?	14
2.9 Hidden Node Problem	14
2.10 Types of Hidden Node Problem	14

2.10(a) Hidden Terminal Problem	15
2.10(b) Exposed Terminal Problem	15
2.11 Solution of Hidden Node Problem	16
2.11(a) Increase Transmitting Power from the Nodes	17
2.11(b) Use Omni-directional Antennas	17
2.11(c) Remove Obstacles	17
2.11(d) Move the Node	17
2.11(e) Use protocol enhancement software	17
2.11(f) Use antenna diversity	18
2.11(g) WiCCP (Wireless Central Coordinated Protocol)	18
2.11(h) Equalizing technology	19
2.12 Advantages of CSMA/CA	20
2.13 Disadvantages of CSMA/CA	20

CHAPTER 3: MACA PROTOCOL 21-47

3.1 What is MACA?	21
3.2 RTS/CTS	23
3.3 What is MACAW?	25
3.4 Principle operation of MACAW	25
3.5 MAC Protocol	27
3.5(a) MAC sub layer	27
3.5(b) Addressing mechanism	28
3.5(c) Channel access control mechanism	29
3.6 Ad hoc network	29
3.7 Classifications of MAC protocols	31
3.8 RTS/CTS Protocol Description	32
3.9 Mechanism of RTS/CTS	33
3.10 Advantages of RTS-CTS mechanism	34
3.11 Disadvantages of RTS-CTS mechanism	34
3.11(a) Inhibiting Non-interfering Parallel Transmission	35
3.11(b) False Blocking	35
3.11(c) Virtual Jamming	35
3.12 CSMA/CA (used in IEEE 802.11/WiFi WLANs)	35

3.13 IEEE 802.11 RTS/CTS Exchange	36
3.14 RTS/CTS HANDSHAKE with ACK	37
3.15 IEEE 802.11 RTS/CTS	37
3.16 The IEEE 802.11 standard	38
3.17 Frame Format of IEEE 802.11 RTS/CTS	39
3.18 RTS/CTS with Three Way Handshaking Protocol	41
3.19 Three Way Handshake	42
3.20 Three Way Handshaking Protocol	44
3.21 TCP Three Way Handshake	44
3.22 TCP Segment Structure	47
CHAPTER 4: VALIDATION BY SIMULATION	48-52
4.1 Network Simulator 2	48
4.2 Experimental Setup	48
4.3 Working Procedure	49
4.4 Simulation Parameters	51
CHAPTER 5: CONCLUSION	53
5.1 Conclusion	53
5.2 Future Works	53
REFERENCE	54

LIST OF FIGURE

FIGURE NO	TITLE	PAGES
2.1	CSMA/CA channel Access Mechanisms	4
2.2	Simplified Algorithm of CSMA/CA	7
2.3	Flowchart for CSMA/CA as used in wireless LANs	8
2.4	CSMA/CA and NAV	9
2.5	CSMA/CA Protocol	10
2.6	The Hidden Node Problem	14
2.7	Hidden Terminal Problem	15
2.8	Exposed Terminal Problem	16
3.1	RTS/CTS with MACA	23
3.2	RTS/CTS Graphical figure	24
3.3	An example to illustrate the principle of MACAW	26
3.4	RTS/CTS Mechanism	33
3.5	RTS/CTS HANDSHAKE with ACK	37
3.6	IEEE 802.11 standard's network topology	39
3.7	Hidden Station Problem	41
3.8	Exposed Station Problem	42
3.9	Establish Three Way Handshaking	43
3.10	TCP Segment Structure	47
4.1	Simulation Topology	49
4.2	Line Connectivity Graph	50
4.3	Result	50
4.4	Data packet analysis.....	51

LIST OF TABLE

TABLE NO	TITLE	PAGES
4.1	Simulation parameter of data transmission	51
4.2	Data comparison of packet analysis	52

Chapter: 01

INTRODUCTION

1.1 General Introduction

In the CSMA/CA wireless networks, the collision avoidance mechanism is severely affected by hidden terminal problem and frequency of packet collision increases. However, the detailed analysis of the packet transmission success ratio suffered from hidden terminals in fading environment has not been studied. This paper presents the method for analyzing the ratio by setting a mathematical model while considering three parameters: distances, propagation characteristic of radio wave and carrier sense level. The network simulations for the same model were conducted for validation. The results show that the carrier sense level has significant impact on the packet transmission performance. CSMA/CA protocols rely on the random deferment of packet transmissions. Like most other protocols, CSMA/CA was designed with the assumption that the nodes would play by the rules. This can be dangerous, since the nodes themselves control their random deferment. Indeed, with the higher programmability of the network adapters, the temptation to tamper with the software or firmware is likely to grow; by doing so, a user could obtain a much larger share of the available bandwidth at the expense of other users. We use a game-theoretic approach to investigate the problem of the selfish behavior of nodes in CSMA/CA networks, specifically geared towards the most widely accepted protocol in this class of protocols, IEEE 802.11. An enhanced CSMA/CA protocol to be used in the Medium Access Control (MAC) layer of the IEEE 802.11 standard for wireless local area networks (wireless LANs) is proposed in this work. In wireless LANs, the CSMA/CA protocol supports asynchronous data transfer, and adopts an acknowledgement mechanism to confirm successful transmissions and a Three Way Handshaking mechanism to reduce collisions. In both cases, a binary exponential back-off mechanism is used. The enhanced protocol improves the exponential back-off scheme by dynamically adjusting the contention window (CW) around the optimal value.

In this report to realize the multi-user multiple input multiple output (MIMO) advantage over WLANs, it requires significant changes in the MAC protocol. Either the dominant MAC protocol carrier sense multiple access/collision avoidance (CSMA/CA) needs to be replaced by a novel multi-user MIMO aware MAC protocol or it should be upgraded into

multi-user MIMO aware CSMA/CA. Nevertheless, the simplest approach would be upgrading the CSMA/CA. Simple modifications in the control packets format and/or the channel access mechanism can upgrade CSMA/CA into simple, yet practicable, multi-user MIMO aware MAC protocol. By utilizing convenient changes, several modification approaches can be provisioned for this purpose. Hence, it is important to understand their performance benefits and trade-offs. In this article, we discuss some of such modification approaches that best represent the possible modifications. We provide their detail performance analysis based on analytical modeling and derived expressions in terms of throughput and delay. We also derive expressions for achievable performance and present their performance limits too. It has been shown that CSMA-type random access algorithms can achieve the maximum possible throughput in ad hoc wireless networks. However, these algorithms assume an idealized continuous-time CSMA protocol where collisions can never occur. In addition, simulation results indicate that the delay performance of these algorithms can be quite bad. On the other hand, although some simple heuristics (such as distributed approximations of greedy maximal scheduling) can yield much better delay performance for a large set of arrival rates, they may only achieve a fraction of the capacity region in general.

1.2 Goal of the research work

This thesis focuses on the hidden node moving in three way handshaking protocol. The details of the implementation of hidden node moving in network simulator (NS2) will be presented. It includes the definition of various service flows defined by the IEEE 802.11 standard. The IEEE 802.11 standard defines the protocol for two types of networks: Ad-hoc networks and client/server networks. The details of the network's OSI layer three way handshaking implementation are presented. To analyze the three way handshaking simulation based on the network simulator (NS2) is used. The goal is to compare different types of service flows with respect to the three way handshaking protocols, such as, throughput, average jitter, average delay and packet loss.

1.3 Organization of the thesis

The first chapter of this thesis gives a brief introduction to CSMA/CA. IEEE 802.11 standard is presented. MAC layer, CW and Three Way Handshaking is presented this

chapter. This is followed by the problem statement and the contributions of this thesis are documented.

The second chapter presents details of the CSMA/CA mechanism, algorithm and flowchart. CSMA/CA protocol is implemented in the wireless networks using three basic techniques. This chapter describes basic of the hidden node.

The third chapter presents MACA protocol, MACAW, MAC protocol. The IEEE 802.11 standard is implemented this chapter. This chapter also describes TCP Three Way Handshaking.

Chapter four describes the simulation set up, the simulation environment used where NS2 is used. The parameters that indicate NS2 are described in details. This chapter also presents the results obtained. The hidden node move that indicate TCP/IP are studied for various use cases and compare the output result.

The last chapter presents the conclusions from the work performed and also gives insight into the future work.

Chapter: 2

CSMA/CA

2.1 Overview of CSMA/CA

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is the channel access mechanism used by most wireless LANs in the ISM bands. A channel access mechanism is the part of the protocol which specifies how the node uses the medium: when to listen, when to transmit.

The basic principles of CSMA/CA are listening before talk and contention. This is an asynchronous message passing mechanism (connectionless), delivering a best effort service, but no bandwidth and latency guarantee. It's main advantages are that it is suited for network protocols such as TCP/IP, adapts quite well with the variable condition of traffic and is quite robust against interferences. CSMA/CA is fundamentally different from the channel access mechanism used by cellular phone systems. CSMA/CA is derived from CSMA/CD (Collision Detection), which is the base of Ethernet. The main difference is the collision avoidance: on a wire, the transceiver has the ability to listen while transmitting and so to detect collisions (with a wire all transmissions have approximately the same strength). But, even if a radio node could listen on the channel while transmitting, the strength of its own transmissions would mask all other signals on the air. So, the protocol can't directly detect collisions like with Ethernet and only tries to avoid them.

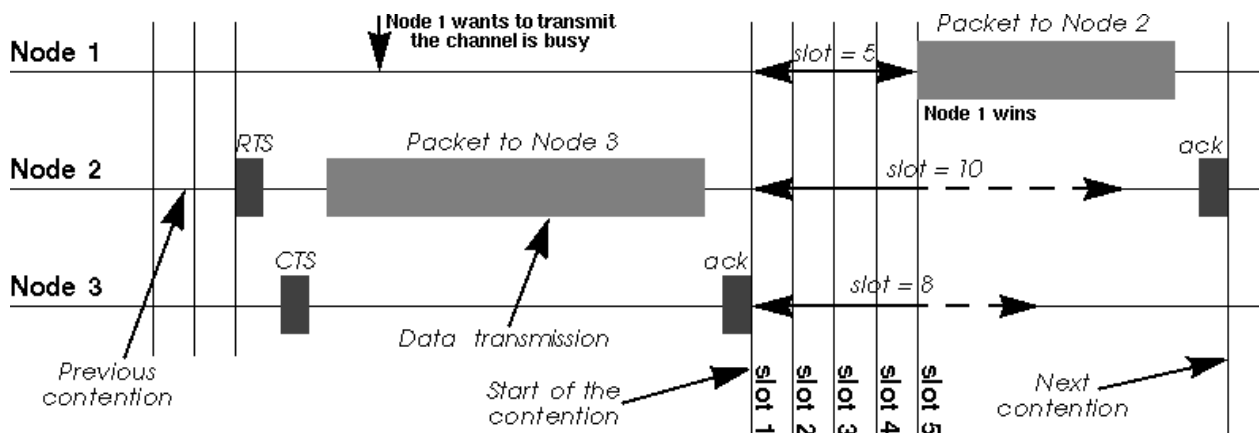


Figure 2.1: CSMA/CA channel Access Mechanisms

The protocol starts by listening on the channel (this is called carrier sense), and if it is found to be idle, it sends the first packet in the transmit queue. If it is busy (either another node transmission or interference), the node waits the end of the current transmission and then starts the contention (wait a random amount of time). When its contention timer expires, if the channel is still idle, the node sends the packet. The node having chosen the shortest contention delay wins and transmits its packet. The other nodes just wait for the next contention (at the end of this packet). Because the contention is a random number and done for every packets, each node is given an equal chance to access the channel (on average - it is statistic). As we have mentioned, we can't detect collisions on the radio, and because the radio needs time to switch from receive to transmit, this contention is usually slotted (a transmission may start only at the beginning of a slot: 50 μ s in 802.11 FH and 20 μ s in 802.11 DS). This makes the average contention delay larger, but reduces significantly the collisions (we can't totally avoid them). [1]

2.2 What is CSMA/CA?

Carrier sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle". When they do transmit, nodes transmit their packet data in its entirety.

It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is unreliable due to the hidden node problem. CSMA/CA is a protocol that operates in the Data Link Layer (Layer 2) of the OSI model.

In Carrier Sense Multiple Access:

1. If the channel is idle then transmit.
2. If the channel for communication is free then it is going to transmit without any precaution that there might be collision.
3. If the channel is busy, wait for a random time.
4. Waiting time is calculated using Truncated Binary Exponential Back-off (BEB) algorithm.

2.2(a) Binary Exponential Back-off Algorithm:

Exponential back-off is an algorithm that uses feedback to multiplicatively decrease the rate of some process, in order to gradually find an acceptable rate. In a variety of computer networks, binary exponential back-off or truncated binary exponential back-off refers to an algorithm used to space out repeated retransmissions of the same block of data, often as part of network congestion avoidance.

Examples are the retransmission of frames in carrier sense multiple access with collision avoidance (CSMA/CA) and carrier sense multiple access with collision detection (CSMA/CD) networks, where this algorithm is part of the channel access method used to send data on these networks. In Ethernet networks, the algorithm is commonly used to schedule retransmissions after collisions. The retransmission is delayed by an amount of time derived from the slot time and the number of attempts to retransmit.

In computer networking, Carrier Sense Multiple Access with Collision Avoidance and Resolution using Priorities (CSMA/CARP) is a channel access method. CSMA/CARP is similar in nature to the CSMA/CD Channel access method used in Ethernet networks, but CSMA/CARP provides no detection of network collisions. Instead of detecting network collisions, CSMA/CARP attempts to avoid collisions by using a system of transmission priorities. Again, CSMA/CARP is similar to the functions of the CSMA/CA. However, the CSMA/CA (Collision Avoidance) employs a different approach of how to make packets get transmitted over the wire or medium without any difficulties. It is a discrete-time version of the CSMA algorithm. The algorithm generates collision-free transmission schedules while explicitly taking collisions into account during the control phase of the protocol, thus relaxing the perfect CSMA assumption. More importantly, the algorithm allows us to incorporate mechanisms which lead to very good delay performance while retaining the throughput-optimality property. It also resolves the hidden and exposed terminal problems associated with wireless networks.

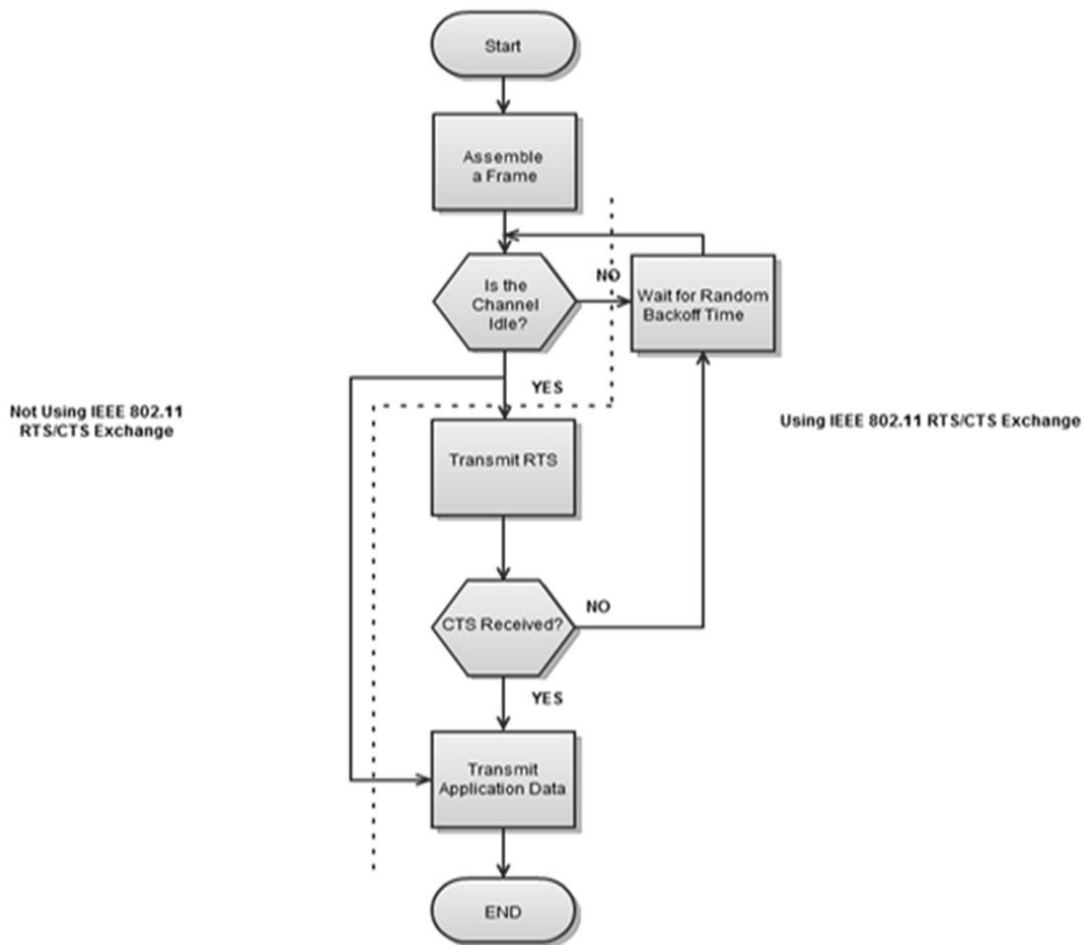


Figure 2.2: Simplified Algorithm of CSMA/CA

.2.3 Flowchart of CSMA/CA:

Figure 2.3 Shows the flow chart explaining the principle of CSMA/CA.

- This is the CSMA protocol with collision avoidance.
- The station ready to transmit, senses the line by using one of the persistent strategies.
- As soon as it find the line to be idle, the station waits for an IFG (Interframe gap) amount of time.
- It then waits for some random time and sends the frame.
- After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.

- If the acknowledgement is received before expiry of the timer, then the transmission is successful.
- But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and resenses the line. [2]

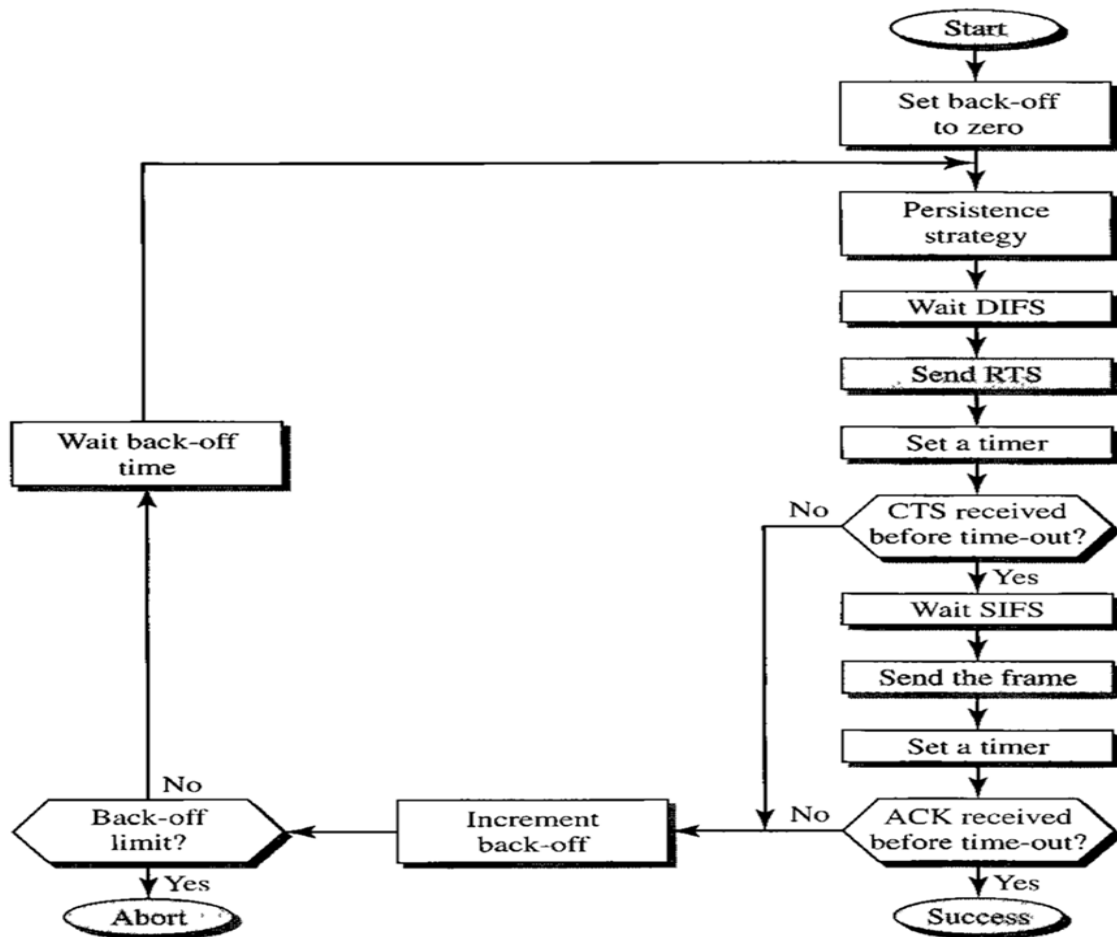


Figure 2.3: Flowchart for CSMA/CA as used in wireless LANs.

2.3(a) Frame Exchange Time Line:

The Figure 2.4 shows the exchange of data and control frames in time.

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
 - The channel uses a persistence strategy with back-off until the channel is idle.

- After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

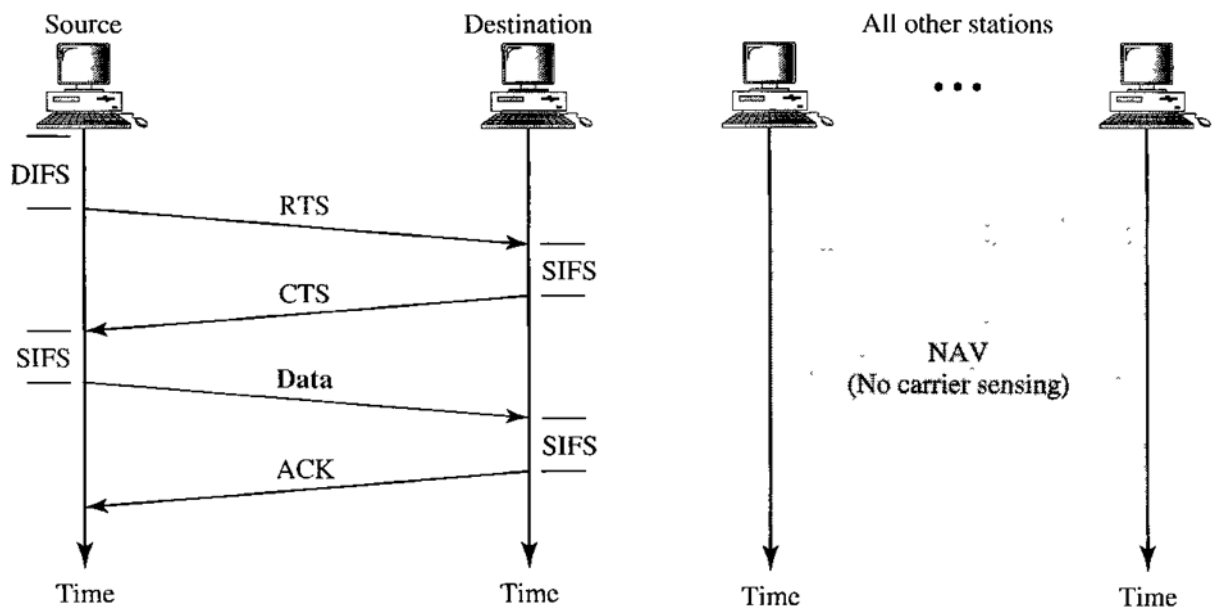


Figure 2.4: CSMA/CA and NAV

3. The source station sends data after waiting an amount of time equal to SIFS.

4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in CSMA/CD is a kind of indication to the some that data have arrived.

2.3(b) Network Allocation Vector (NAV):

Network Allocation Vector When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how

much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV. In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired. In IEEE 802.11 standard, the contention window (CW) sizes are not efficient because it does not consider the system load. There has been several mechanisms to achieve the maximum throughput by the optimal CW. But some parameters such as the number of stations and system utilization are difficult to measure in WLAN systems. To solve this problem, we use the network allocation vector (NAV) which represents the transmission of other stations. This parameter can be used to measure the system load. Thus, the CW sizes can be estimated by the system load. In this paper, we derive the analytical model for the optimal CW sizes and the maximum throughput using the NAV and show the relationships between the CW sizes, the throughput and the NAV. The proposed protocol is designed and implemented in NS2. The simulation has shown significant improvement over slotted and un-slotted CSMA/CA based upon some performance parameters.

2.4 CSMA/CA Protocol:

CSMA/CA protocol is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.

- CSMA/CA avoids the collisions using three basic techniques.

1. Interframe space
2. Contention window
3. Acknowledgements

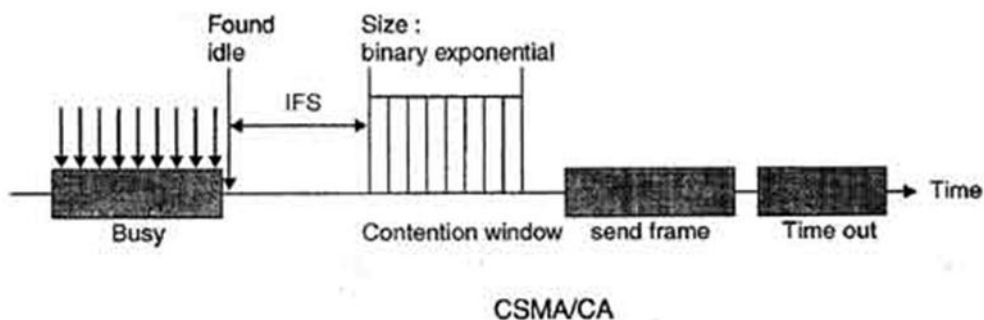


Figure 2.5: CSMA/CA Protocol.

1. Interframe Space (IFS)

- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).
- When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.
- If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.
- IFS variable can also be used to define the priority of a station or a frame.

2. Contention Window

- Contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.
- In contention window the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

3. Acknowledgement

- Despite all the precautions, collisions may occur and destroy the data.
- The positive acknowledgment and the time-out timer can help guarantee that receiver has received the frame.

2.5 Usage of CSMA/CA

- * GNET - an early proprietary LAN protocol
- * Apple's Local Talk implemented CSMA/CA on an electrical bus using a three-byte Jamming signal.
- * 802.11 RTS/CTS implements virtual carrier sensing using short request to send and clear to send messages for WLANs (802.11 mainly relies on physical carrier sensing though).
- * IEEE 802.15.4 (Wireless PAN) uses CSMA/CA
- * NCR Wave LAN - an early proprietary wireless network protocol
- * Home PNA
- * Bus networks
- * The ITU-T G.hn standard, which provides a way to create a high-speed (up to 1 Gigabit/s) local area network using existing home wiring (power lines, phone lines and coaxial cables), uses CSMA/CA as a channel access method for flows that don't require guaranteed quality of service, specifically the CSMA/CARP variant.

2.6 CSMA/CA uses Wireless LAN:

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is the channel access mechanism used by most wireless LANs in the ISM bands. One of the major protocols used for wireless LAN is the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which is a variation of CSMA/CD. Collision avoidance is used to improve the performance of the CSMA method by attempting to divide the channel somewhat equally among all transmitting nodes within the collision domain. [3]

1. Carrier Sense: prior to transmitting, a node first listens to the shared medium (such as listening for wireless signals in a wireless network) to determine whether another node is transmitting or not. Note that the hidden node problem means another node may be transmitting which goes undetected at this stage.

2. Collision Avoidance: if another node was heard, we wait for a period of time for the node to stop transmitting before listening again for a free communications channel.

2.7 Why uses WLAN (Wireless Local Area Network) in CSMA/CA?

- CSMA/CA operates by sensing the state of the medium in order to prevent or recover from a collision. A collision happens when two transmitters transmit at the same time. The data gets scrambled, and the receivers would not be able to discern one from the other thereby causing the information to get lost. The lost information needs to be resent so that the receiver will get it.

- CSMA/CA does not deal with the recovery after a collision. It checks whether the medium is in use or not. If it is busy, then the transmitter waits until it is idle state, before it starts transmitting data. This effectively minimizes the possibility of collisions and makes more efficient use of the medium.

- CSMA/CA reduces the possibility of a collision it is used in wireless network while CSMA/CD only minimizes the recovery time after collision which will occur frequently in wired network so this CSMA/CD helps here better.

Wireless environment is completely different than wired. Different needs, different operation and procedures. The biggest reason for using different algorithm (ca in this case) is the problem of the hidden node. In short it's when a node is not visible (out of range) by an access point, but at the same time visible by other AP. Something like this:

The Hidden Node problem is shown in Figure 2.6 above. Node C cannot hear node A. So if node A is transmitting, node C will not know and may transmit as well. This will result in collisions. The solution to this problem is Carrier Sense Multiple Access with Collision Avoidance or CSMA/CA. CSMA/CA works as follows: the station listens before it sends. If someone is already transmitting, wait for a random period and try again.

If no one is transmitting then it sends a short message. This message is called the Ready To Send message (RTS). This message contains the destination address and the duration of the transmission.

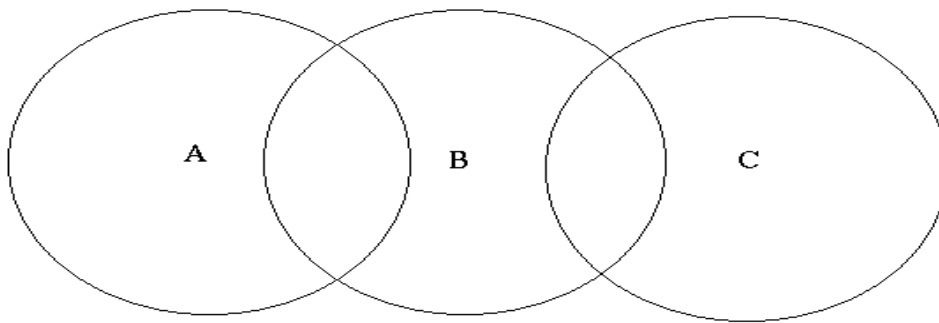


Figure 2.6: The Hidden Node Problem

Other stations now know that they must wait that long before they can transmit. The destination then sends a short message which is the Clear To Send message (CTS). This message tells the source that it can send without fear of collisions. Each packet is acknowledged.

2.8 What is Hidden Node?

In a wireless network nodes can be hidden from each other if they are in communication with a central station but not directly with each other. The presence of hidden nodes creates complications for transmitting throughout the network, and also when two or more networks are trying to share the same frequency and physical space. There are two types of node. Hidden node and Exposed node.

2.9 Hidden Node Problem

The hidden node problem can be observed easily in widespread (>50m radius) WLAN setups with many nodes that use directional antennas and have high upload. This is why IEEE 802.11 is suited for bridging the last mile, for broadband access, only to a very limited extent. Newer standards such as Wi-MAX assign time slots to individual stations, thus preventing multiple nodes from sending simultaneously and ensuring fairness, even in oversubscription scenarios.

2.10 Types of Hidden Node Problem

Hidden Node Problem is Two Types. They are:

- (a) Hidden Terminal Problem

(b) Exposed Terminal Problem

2.10(a) Hidden Terminal Problem

The notorious hidden node problem deals with a configuration of three nodes, like A, B, and C in Figure 2.7. Where by B is within the transmission range of A and C, while C is outside the range of A. In a situation like this, C will not be able to detect problem the ongoing transmission of A to B by carrier sensing and consequently, it can inadvertently interfere with B's reception

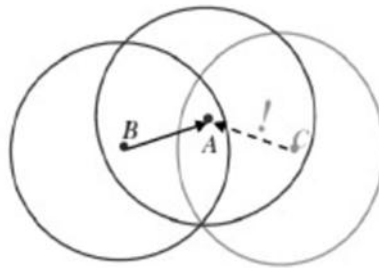


Figure 2.7: Hidden Terminal Problem

of A's packet [1]. The transmission range of a node A is defined as the area inside which other nodes are able to correctly receive A's packets. On the other hand, the carrier sense range of A is the area encompassing those nodes whose transmission A can perceive (carrier sense) while not necessarily being able to receive the transmitted packets [1]. Generally, it is unreasonable to assume that the two areas are always the same, e.g., the carrier sense range can be twice the transmission range [7]. Suppose that every node in Figure 2.7 has the same transmission range (represented by a solid circle). Node C is out of the transmission range of node A and thus would appear as a hidden node to A. However, if the carrier sense range of C is larger than the transmission range of A (see the dashed circle), C is no more hidden because it can sense the transmission of A and thus avoid interfering with it.

2.10(b) Exposed Terminal Problem

In wireless networks, the Exposed Node Problem occurs when a node is prevented from sending packets to other nodes due to a neighboring transmitter. Consider an example of 4 nodes labeled R1, S1, S2, and R2, where the two receivers are out of range of each

other, yet the two transmitters in the middle are in range of each other as shown in Figure 2.8

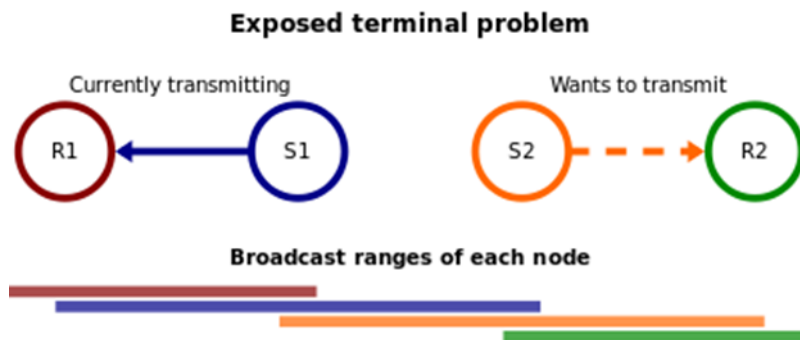


Figure 2.8: Exposed Terminal Problem

Here, if a transmission between node S1 and node R1 is taking place, node S2 is prevented from transmitting to node R2 as it concludes after carrier sense that it will interfere with the transmission by its neighbor node S1. However note that node R2 could still receive the transmission from node S2 without interference because it is out of range from node S1 [6].

2.11 Solution of Hidden Node Problem

The other methods that can be employed to solve hidden node problem are:

- (a) Increase transmitting power from the nodes.
- (b) Use Omni-directional antennas.
- (c) Remove obstacles.
- (d) Move the node.
- (e) Use protocol enhancement software.
- (f) Use antenna diversity.
- (g) Wireless Central Coordinated Protocol.
- (h) Equalizing technology

2.11(a) Increase Transmitting Power from the Nodes

Increasing the power (measured in mWatts) of the nodes can solve the hidden node problem by allowing the cell around each node to increase in size, encompassing all of the other nodes. This configuration enables the non-hidden nodes to detect, or hear, the hidden node. If the non-hidden nodes can hear the hidden node, the hidden node is no longer hidden. Because wireless LANs uses the CSMA/CA protocol, nodes will wait for their turn before communicating with the access point.

2.11(b) Use Omni-directional Antennas

Since nodes using directional antennas are nearly invisible to nodes that are not positioned in the direction the antenna is aimed at, directional antennas should be used only for very small networks (e.g., dedicated point-to-point connections). Use Omni-directional antennas for widespread networks consisting of more than two nodes.

2.11(c) Remove Obstacles

Increasing the power on mobile nodes may not work, if for example, the node that is hidden is that hiding behind a cement or steel wall preventing communication with other nodes. It is doubtful that one would be able to remove such an obstacle, but removal of the obstacle is another method of remedy for the hidden node problem. Keep these types of obstacles in mind when performing a site survey [2].

2.11(d) Move the Node

Another method of solving the hidden node problem is moving the nodes so that they can all hear each other. If it is found that the hidden node problem is the result of a user moving his computer to an area that is hidden from the other wireless nodes, it may be necessary to have that user move again. The alternative to forcing users to move is extending the wireless LAN to add proper coverage to the hidden area, perhaps using additional access points.

2.11(e) Use protocol enhancement software

There are several software implementations of additional protocols that essentially implement a polling or token passing strategy. Then, a master (typically the access point)

dynamically polls clients for data. Clients are not allowed to send data without the master's invitation. This eliminates the hidden node problem at the cost of increased latency and less maximum throughput.

2.11(f) Use antenna diversity

Antenna Diversity is a transmission method using more than one antenna to receive or transmit signals along different propagation paths to compensate for multipath interferences. Due to multipath propagation interference effects between network nodes, the receive signal strength may strongly vary, even for small changes of the propagation conditions, affecting the link quality. These fading effects can result in an increased error floor or loss of the connection between devices. Applying Antenna Diversity transmission techniques in such scenarios improves the reliability of an RF connection between network nodes.

2.11(g) WiCCP (Wireless Central Coordinated Protocol)

WiCCP is a protocol booster for 802.11b DCF based wireless networks that provides cyclic token-passing medium access, and scheduled allocation of the available network resources,

Eliminating the "Hidden Node" problem. It is a pure kernel implementation resulting in high efficiency traffic control. It's not required extra configuration e.g. static ARP tables or dedicated routing contexts. WiCCP can be used in fixed wireless network deployments. It is interesting to note under what conditions WiCCP will work, and when it will not work - at least optimally. WiCCP will outperform systems that do not run it when the utilization of the bandwidth increases above some high percentage. If we are running standard Ethernet utilization would be about 80%. Above this percentage of utilization, whatever that is, the channel assignment ability of WiCCP will allow the utilization to increase almost to 100% or at least as close as is humanly possible [9]. Looking on the other end of the scale, standard 802.11b will work best when the utilization is low, and the levels are set correctly so that at the access point all power level are the same. Under low utilization it is likely that the power levels do not affect things too much. The main question is regarding heavy traffic. WiCCP allows a guarantee of bandwidth for a particular user and this solution appears to be the correct solution for this case to solve this problem. The ability to offer a guarantee and then offer more on top of

that where available is worthwhile. The problem is the overhead of polling. As the number of users increases, WiCCP will tend to have issues with assigning timeslots to each, ensuring latency. Standard 802.11b will have a definite advantage when there are a lot of stations, and very few want to transmit most of the time - Such as 50 laptops who only check their mail once every 15 minutes (without reading), as opposed to 50 users attempting to surf the web.[4]

2.11(h) Equalizing technology

Equalizing technology, which is fully compatible with 802.11, works by taking advantage of the natural inclination of Internet connections to back off when artificially restrained.

Equalizing periodically (every second) measures the total aggregate bandwidth throughput traversing the AP. If it is sensed that the upper limit is being reached, the dominating flows will be identified and encouraged to back off by artificially restraining them. This frees up bandwidth for lesser powered remote nodes.

By keeping track of every flow going through the AP, equalizing technology can identify those taking an unequal share of bandwidth and thus crowding out flows from weaker nodes.

Equalizing discriminates detrimental flows by taking the following questions into consideration:

1. How persistent is the flow?
2. How many active flows are there?
3. How long has the flow been active?
4. How much total congestion is currently on the trunk?
5. How much bandwidth is the flow using relative to the link size?

The key to making this happen over 802.11 relies on the fact that if you slow a stream down, the application at the root cause will back off and also slow down. This can be done by the deploying equalizing technology after the access point without any changes to the 802.11 protocol since the throttling is actually done independent of the radio. The

throttling of heavy streams happens between the AP and the connection to the Internet (or other external source).

Traffic equalizing technologies are not universally applicable solutions to the hidden node problem. Rather, they are primarily a pragmatic fix to reduce symptoms without fixing the underlying problem.

2.12 Advantages of CSMA/CA

-Effective: Avoids data collisions.

-Reliable: Intent signals are sent until the cable is clear so that data will travel and reach its destination safely.

2.13 Disadvantages of CSMA/CA

-Relatively slow: A signal of intent must be sent every time a computer wants to transmit causing signal traffic.

-Inappropriate for large/active networks: The slowdown increases, as the network grows larger.

-Limited: suffers from same distance limitations as CSMA/CD since it must listen for the signals of intent.

Chapter: 3

MACA Protocol

3.1 What is MACA?

Multiple Access with Collision Avoidance (MACA) is a slotted media access control (MAC) protocol used in wireless LAN data transmission to avoid collisions caused by the hidden station problem and to simplify exposed station problem.

MULTIPLE ACCESS COLLISION AVOIDANCE (MACA)

- Uses Request-To-Send (RTS) and Clear To-Send (CTS) handshake to reduce the effects of hidden terminals.
- Data transfer duration is included in RTS and CTS, which helps other nodes to be silent for this duration.
- If a RTS/CTS packet collides, nodes wait for a random time which is calculated using BEB algorithm.

The basic idea of MACA is a wireless network node makes an announcement before it sends the data frame to inform other nodes to keep silent. When a node wants to transmit, it sends a signal called Request-To-Send (RTS) with the length of the data frame to send. If the receiver allows the transmission, it replies the sender a signal called Clear-To-Send (CTS) with the length of the frame that is about to receive.

Meanwhile, a node that hears RTS should remain silent to avoid conflict with CTS; a node that hears CTS should keep silent until the data transmission is complete. [5]

WLAN data transmission collisions may still occur, and the MACA for Wireless (MACAW) is introduced to extend the function of MACA. It requires nodes sending acknowledgements after each successful frame transmission, as well as the additional function of Carrier sense.

Distributed, Contention based MAC Protocol

MACA is distributed contention based mac protocol. Basic ideas for a distributed MAC

ALOHA – no good in most cases

Listen before talk (Carrier Sense Multiple Access, CSMA) – better, but suffers from sender not knowing what is going on at receiver, might destroy packets despite first listening for a receiver additionally needs some possibility to inform possible senders in its vicinity about impending transmission (to “shut them up” for this duration). Distributed medium access control (MAC) with QoS provisioning for both single- and multi-hop wireless networks including wireless local area networks (WLANs), wireless ad hoc networks, and wireless mesh networks.

In addition, a novel token-based scheduling scheme is proposed to provide great flexibility and facility to the network service provider for service class management.

Main options to shut up senders –MACA

(a)Receiver informs potential interferers while a reception is on-going

-By sending out a signal indicating just that

Problem: Cannot use same channel on which actual reception takes place

- Use separate channel for signaling

(b)Receiver informs potential interferers before a reception is on-going

-Can use same channel

-Receiver itself needs to be informed, by sender, about impending transmission

-Potential interferers need to be aware of such information, need to store it.

Receiver informs interferers before transmission – MACA

-Sender B asks receiver C whether C is able to receive a transmission

Request to Send (RTS)

-Receiver C agrees, sends out a Clear to Send (CTS)

-Potential interferers overhear either RTS or CTS and know about impending transmission and for how long it will last

Store this information in a Network Allocation Vector

-B sends, C ACKs

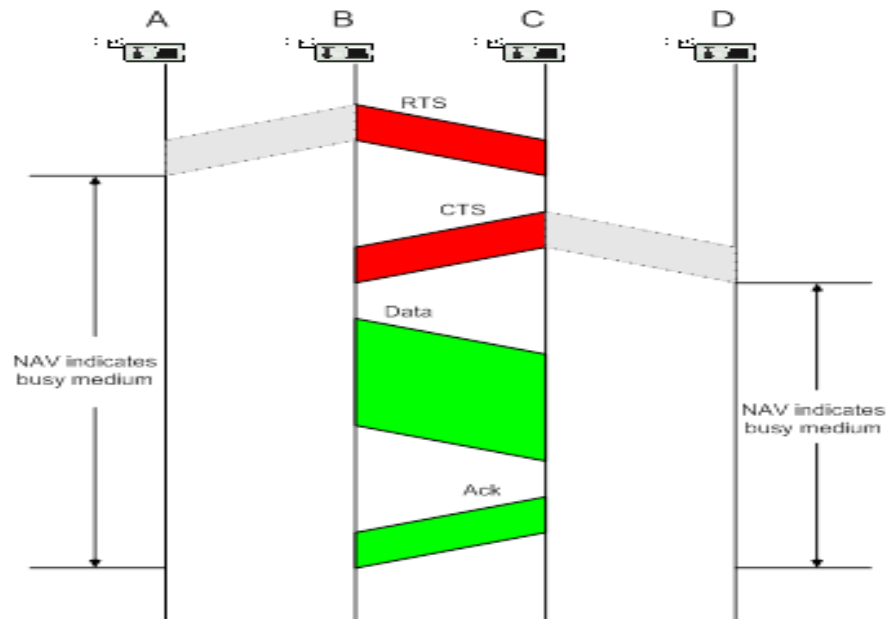


Figure 3.1: RTS/CTS with MACA

3.2 RTS/CTS:

RTS (Request To Send):

Sender asks receiver whether it is able to receive a transmission Request to Send.

CTS (Clear To Send):

Receiver agrees, sends out a transmission Clear to Send.

The hidden node problem comes from the fact that all nodes may not hear each other because the attenuation is too strong between them. Because transmissions are based on the carrier sense mechanism, those nodes ignore each other and may transmit at the same time. Usually, this is a good thing because it allows frequency reuse (they are effectively in different cells). But, for a node placed in between, these simultaneous transmissions

have a comparable strength and so collide (in its receiver). This node could be impossible to reach because of these collisions.

The fundamental problem with carrier sense only is that the transmitter tries to estimate if the channel is free at the receiver with only local information. The situation might be quite different between those two locations. An simple and elegant solution to this problem is to use RTS/CTS (Request To Send/Clear To Send). RTS/CTS is a handshaking: before sending a packet, the transmitter sends a RTS and wait for a CTS from the receiver (see figure 3.2).

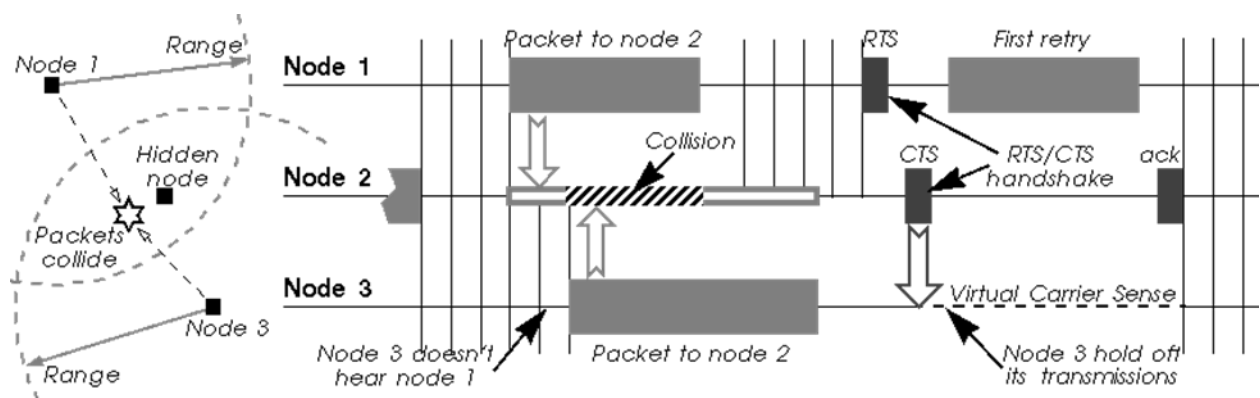


Figure 3.2: RTS/CTS Graphical figure

The reception of a CTS indicates that the receiver is able to receive the RTS, so the packet (the channel is clear in its area).

At the same time, every node in the range of the receiver hears the CTS (even if it doesn't hear the RTS), so understands that a transmission is going on. The nodes hearing the CTS are the nodes that could potentially create collisions in the receiver (assuming a symmetric channel). Because these nodes may not hear the data transmission, the RTS and CTS messages contain the size of the expected transmission (to know how long the transmission will last). This is the collision avoidance feature of the RTS/CTS mechanism (also called virtual carrier sense): all nodes avoid accessing the channel after hearing the CTS even if their carrier sense indicate that the medium is free. [6]

3.3 What is MACAW?

Multiple Access with Collision Avoidance for Wireless (MACAW) is a slotted Medium Access Control (MAC) protocol widely used in ad hoc networks. [2] Furthermore, it is foundation of many other MAC protocols used in Wireless Sensor Networks (WSN).[2] The IEEE 802.11 RTS/CTS mechanism is adopted from this protocol. [4] It uses RTS-CTS-DS-DATA-ACK frame sequence for transferring data, sometimes preceded by an RTS-RRTS frame sequence, in view to provide solution to the hidden terminal problem. Although protocols based on MACAW, such as S-MAC, use carrier sense in addition to the RTS/CTS mechanism, MACAW does not make use of carrier sense.

3.4 Principle operation of MACAW:

An example to illustrate the principle of MACAW. It is assumed that only adjacent nodes are in transmission range of each other. Assume that node A has data to transfer to node B.

Node A initiates the process by sending a Request to Send frame (RTS) to node B. The destination node (node B) replies with a Clear To Send frame (CTS).

After receiving CTS, node A sends data. After successful reception, node B replies with an acknowledgement frame (ACK). If node A has to send more than one data fragment, it has to wait a random time after each successful data transfer and compete with adjacent nodes for the medium using the RTS/CTS mechanism.

Any node overhearing an RTS frame (for example node F or node E in the illustration) refrains from sending anything until a CTS is received, or after waiting a certain time. If the captured RTS is not followed by a CTS, the maximum waiting time is the RTS propagation time and the destination node turnaround time.[1]

Any node (node C and node E) overhearing a CTS frame refrains from sending anything for the time until the data frame and ACK should have been received (solving the hidden terminal problem), plus a random time. Both the RTS and CTS frames contain information about the length of the DATA frame. Hence a node uses that information to estimate the time for the data transmission completion.

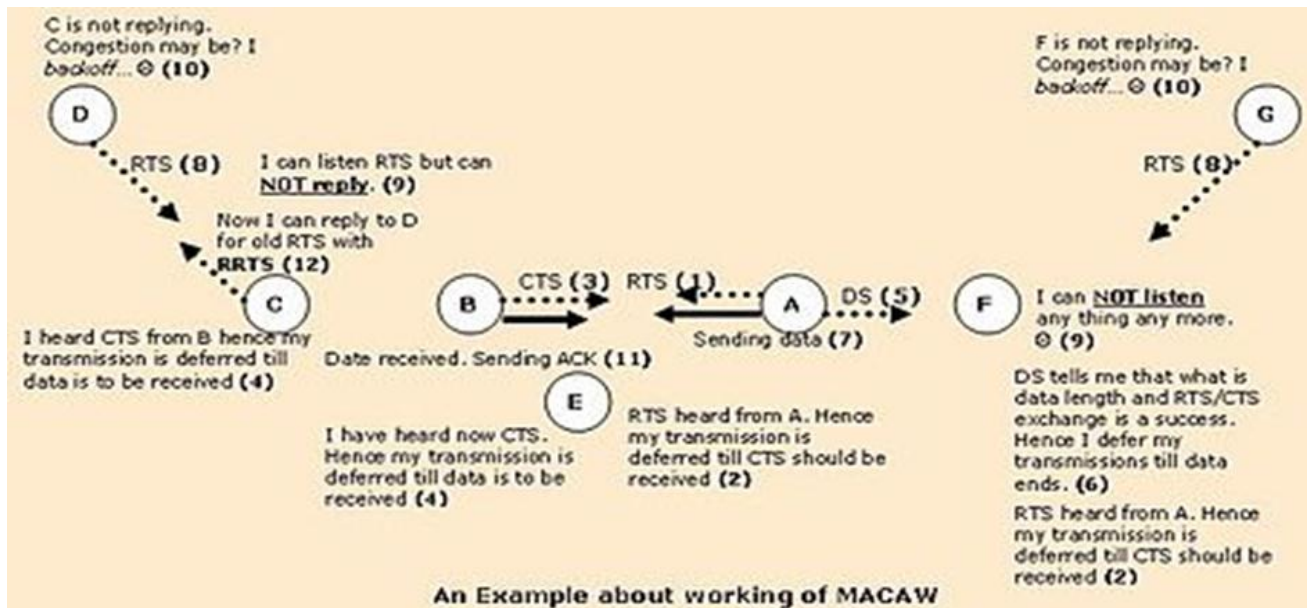


Figure3.3: An example to illustrate the principle of MACAW. It is assumed that only adjacent nodes are in transmission range of each other.

Before sending a long DATA frame, node A sends a short Data-Sending frame (DS), which provides information about the length of the DATA frame. Every station that overhears this frame knows that the RTS/CTS exchange was successful.

An overhearing station (node F), which might have received RTS and DS but not CTS, defers its transmissions until after the ACK frame should have been received plus a random time.[1]

To sum up, a successful data transfer (A to B) consists of the following sequence of frames:

1. "Request To Send" frame (RTS) from A to B
2. "Clear To Send" frame (CTS) from B to A
3. "Data Sending" frame (DS) from A to B
4. DATA fragment frame from A to B, and
5. Acknowledgement frame (ACK) from B to A.

MACAW is a non-persistent slotted protocol, meaning that after the medium has been busy, for example after a CTS message, the station waits a random time after the start of a time slot before sending an RTS. This results in fair access to the medium. If for example nodes A, B and C have data fragments to send after a busy period, they will have the same chance to access the medium since they are in transmission range of each other.

3.5 MAC Protocol

In the seven-layer OSI model of computer networking, media access control (MAC) data communication protocol is a sub layer of the data link layer, which itself is layer 2. The MAC sub layer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a medium access controller.

The MAC sub layer acts as an interface between the logical link control (LLC) sub layer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

3.5(a) MAC sub layer

According to IEEE Std 802-2001 section 6.2.3 "MAC sub layer", the primary functions performed by the MAC layer are:

- * Frame delimiting and recognition
- * Addressing of destination stations (both as individual stations and as groups of stations)
- * Conveyance of source-station addressing information
- * Transparent data transfer of LLC PDUs, or of equivalent information in the Ethernet sublayer
- * Protection against errors, generally by means of generating and checking frame check sequences
- * Control of access to the physical transmission medium

In the case of Ethernet, according to 802.3-2002 section 4.1.4, the functions required of a MAC are:

- * receive/transmit normal frames
- * half-duplex retransmission and backoff functions
- * append/check FCS (frame check sequence)
- * interframe gap enforcement
- * discard malformed frames
- * append(tx)/remove(rx) preamble, SFD (start frame delimiter), and padding
- * half-duplex compatibility: append(tx)/remove(rx) MAC address

3.5(b) Addressing mechanism

The local network addresses used in IEEE 802 networks and FDDI networks are called MAC addresses; they are based on the addressing scheme used in early Ethernet implementations. A MAC address is a unique serial number. Once a MAC address has been assigned to a particular network interface (typically at time of manufacture), that device should be uniquely identifiable amongst all other network devices in the world. This guarantees that each device in a network will have a different MAC address (analogous to a street address). This makes it possible for data packets to be delivered to a destination within a subnetwork, i.e. hosts interconnected by some combination of repeaters, hubs, bridges and switches, but not by network layer routers. Thus, for example, when an IP packet reaches its destination (sub) network, the destination IP address (a layer 3 or network layer concept) is resolved with the Address Resolution Protocol for IPv4, or by Neighbor Discovery Protocol (IPv6) into the MAC address (a layer 2 concept) of the destination host.

Examples of physical networks are Ethernet networks and Wi-Fi networks, both of which are IEEE 802 networks and use IEEE 802 48-bit MAC addresses.

A MAC layer is not required in full-duplex point-to-point communication, but address fields are included in some point-to-point protocols for compatibility reasons.

3.5(c) Channel access control mechanism

The channel access control mechanisms provided by the MAC layer are also known as a multiple access protocol. This makes it possible for several stations connected to the same physical medium to share it. Examples of shared physical media are bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links. The multiple access protocol may detect or avoid data packet collisions if a packet mode contention based channel access method is used, or reserve resources to establish a logical channel if a circuit switched or channelization based channel access method is used. The channel access control mechanism relies on a physical layer multiplex scheme.

The most widespread multiple access protocol is the contention based CSMA/CD protocol used in Ethernet networks. This mechanism is only utilized within a network collision domain, for example an Ethernet bus network or a hub-based star topology network. An Ethernet network may be divided into several collision domains, interconnected by bridges and switches. A multiple access protocol is not required in a switched full-duplex network, such as today's switched Ethernet networks, but is often available in the equipment for compatibility reasons.

3.6 Ad hoc network

A wireless ad hoc network is a decentralized type of wireless network. [6] The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks. It also refers to a network device's ability to maintain link status information for any number of devices in a 1-link (aka "hop") range, and thus, this is most often a Layer 2 activity.

Because this is only a Layer 2 activity, ad hoc networks alone may not support a routable IP network environment without additional Layer 2 or Layer 3 capabilities.

Technical requirements

An ad hoc network is made up of multiple “nodes” connected by “links.”

Links are influenced by the node's resources (e.g., transmitter power, computing power and memory) and behavioral properties (e.g., reliability), as well as link properties (e.g. length-of-link and signal loss, interference and noise). Since links can be connected or disconnected at any time, a functioning network must be able to cope with this dynamic restructuring, preferably in a way that is timely, efficient, reliable, robust, and scalable. The network must allow any two nodes to communicate by relaying the information via other nodes. A “path” is a series of links that connects two nodes. Various routing methods use one or two paths between any two nodes; flooding methods use all or most of the available paths.[5]

Mathematical models

In recent years mathematical models have been proposed to study various types of wireless ad hoc networks. One class of models involves using stochastic processes to represent the placement of the nodes in the ad hoc network. More specifically, stochastic geometry models of wireless networks have been proposed and studied.

Medium-access control

In most wireless ad hoc networks, the nodes compete for access to shared wireless medium, often resulting in collisions (interference). Using cooperative wireless communications improves immunity to interference by having the destination node combine self-interference and other-node interference to improve decoding of the desired signal.

3.7 Classifications of MAC protocols

MAC protocols for ad hoc wireless networks can be classified into several categories based on various criteria such as initiation approach, time synchronization, and reservation approach. Ad hoc network MAC protocols can be classified into three basic types,

Contention based protocols.

Contention based protocols with reservation mechanism.

Contention based protocols with scheduling mechanism.

Apart from these, there exist other MAC protocols that can't be classified clearly under any one of the above three types.

Contention Based Protocols

These protocols follow a contention based channel access policy. A node does not make any resource reservation in priori. Whenever it receives a packet to be transmitted, it contends with other nodes for access to the shared channel. This system can't provide QoS guarantee to session since nodes are not guaranteed regular access to the channel.

They are further divided in two types,

- Sender initiated protocols. Packet transmission are initiated by sender node.

-Receiver initiated protocols. The receiver node initiates the contention resolution protocol.

Sender initiated protocols are further divided into two types,

- Single channel sender initiated protocols. Here the total available bandwidth is used as it is, without being divided. A node that wins the contention to the channel can make use of the entire bandwidth.

-Multichannel sender initiated protocols. Here the available bandwidth is divided into multiple channels. This enables several nodes to simultaneously transmit data, each using a separate channel. Some protocols dedicate a frequency channel exclusively for transmitting control information.

Contention Based Protocols with Reservation Mechanisms

Ad hoc wireless networks sometimes may need to support real time traffic, which requires QoS guarantees to be provided. In order to support such traffic, certain protocols have mechanisms for reserving bandwidth in priori. Such protocols can guarantee QoS to time sensitive traffic sessions. These protocols are classified into two types,

- **Synchronous protocols:** These systems require time synchronization among all the nodes in the network, so that reservation made by a node are known to other nodes in its neighborhood. Global time synchronization is difficult to achieve.
- **Asynchronous protocols:** They do not require any global synchronization among the nodes. These protocols usually use relative time information for effecting reservations.

Contention Based Protocols with Scheduling Mechanisms

These protocols focus on packet scheduling at nodes, and also scheduling nodes for access to the channel. Node scheduling is done in a manner so that all nodes are treated fairly. Scheduling based schemes are also used for enforcing priorities among flows whose packets are queued at nodes. Some scheduling schemes also take into consideration battery characteristics, such as remaining battery power, while scheduling nodes for access to the channel.

3.8 RTS/CTS Protocol Description

The RTS Threshold (RT) value which determines when the RTS/CTS handshaking mechanism should be used is an important parameter to investigate; since different RTS-Threshold values will produce different performance characteristics in data transmission. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of the network packet. However, the more RTS packets that are sent, the quicker the system can recover from interference or collisions as would be the case in a heavily loaded network, or a wireless network with much electromagnetic interference.

3.9 Mechanism of RTS/CTS:

A node wishing to send data initiates the process by sending a Request to Send frame (RTS). The destination node replies with a Clear To Send frame (CTS). Any other node receiving the RTS or CTS frame should refrain from sending data for a given time (solving the hidden node problem). The amount of time the node should wait before trying to get access to the medium is included in both the RTS and the CTS frame. This protocol was designed under the assumption that all nodes have the same transmission range.[7]

RTS/CTS is an additional method to implement virtual carrier sensing in Carrier sense multiple access with collision avoidance (CSMA/CA).

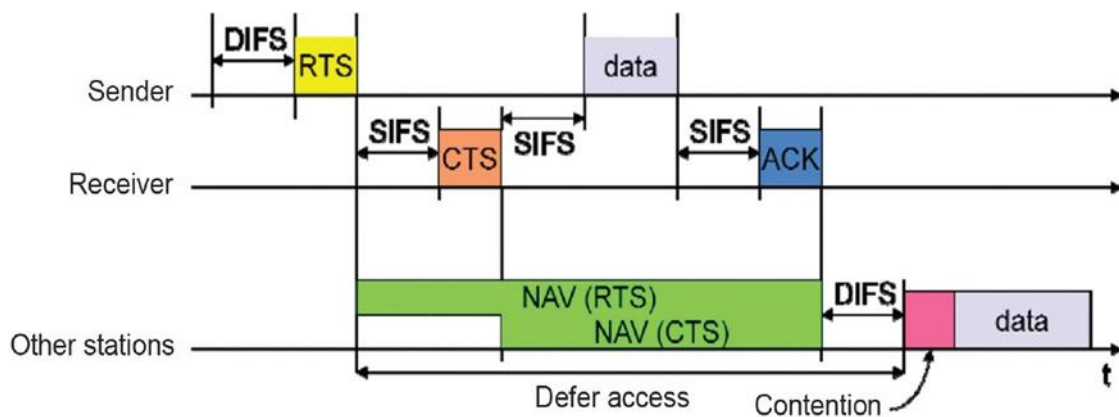


Figure3.4: RTS/CTS Mechanism

By default, 802.11 relies on physical carrier sensing only which is known to suffer from the hidden terminal problem.

DCF Medium Access Mechanism

The DCF is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) where carrier sensing is done by physical sensing and virtual sensing. Both sensing mechanisms are used to determine the state of the medium. For physical carrier sensing traditional CSMA/CA, as shown in Fig: 3.3 is used. It requires the nodes to first sense the channel to check whether it is idle for a DCF Inter-frame Space (DIFS) interval, then attempts packet transmission. On the other hand, for virtual carrier sensing (VCS), RTS/CTS handshake and Network Allocation Vector (NAV) scheme is used as shown in Fig: 3.3. The Virtual Carrier Sensing employs RTS/CTS packets exchange for channel

reservation. The sender transmits a Request-To-Send frame to its receiver. The receiver sends a Clear-To-Send frame if the NAV at the receiver indicates idle channel. Then the sender transmits the DATA frame and waits for acknowledgment ACK.

3.10 Advantages of RTS-CTS mechanism

To alleviate hidden node problem, Two way handshaking protocol known as the RTS/CTS handshaking mechanism. An improved protocol which is known as RTS-CTS-DATA-ACK handshaking mechanism.

The advantages of this mechanism are

To reduce frame collisions introduced by the hidden terminal problem.

Originally the protocol fixed the exposed terminal problem as well, but modern RTS/CTS includes ACKs and does not solve the exposed terminal problem. This mechanism helps to solve this problem only if the nodes are synchronized. When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an exposed node and is permitted to transmit to other neighboring nodes.

It lowers the overhead of a collision on the medium (collisions are much shorter in time). If two nodes attempt to transmit in the same slot of the contention window, their RTS collide and they don't receive any CTS, so they lose only a RTS, whereas in the normal scenario they would have lost a whole packet. Because the RTS/CTS handshaking adds a significant overhead, usually it is not used for small packets or lightly loaded networks.

3.11 Disadvantages of RTS-CTS mechanism

Though the RTS/CTS mechanism is able to solve the hidden node problem and reduce packet collision probability, it has several disadvantages. Authors have discussed several of these disadvantages like Inhibiting non-interfering parallel transmission, False Blocking & and Virtual Jamming.

3.11(a) Inhibiting Non-interfering Parallel Transmission

RTS/CTS mechanism blocks some non-interfering transmission which would be possible with the basic mechanism without collision. Thus, it will cause the reduction of overall throughput.

3.11(b) False Blocking

In the false blocking problem a node can remain blocked during the whole interval of a non-existing conversation. The worse fact is that, it can trigger a chain of nodes to be blocked by the non-existing conversation.

3.11(c) Virtual Jamming

In the virtual jamming problem, a potential malicious node, can make use of the false blocking problem by sending short RTS packets in short periods virtually jamming the whole or a significant part of the network using relatively small power.

From the above discussion, we can realize that the RTS/CTS-based reservation scheme trades some problems (like the hidden node problem) for others (inhibition of parallel transmissions and exposure to virtual jamming attacks). While elimination of the interference caused by hidden nodes does have a positive impact on the network performance, the problems introduced by the RTS/CTS mechanism will tend to counterbalance those benefits. Therefore we need to continue with the both schemes (i.e. the basic scheme and the RTS/CTS based scheme) in a balanced way to reduce the probability of collision and at the same time to avoid the problems of RTS/CTS mechanism. This balance can be achieved if we can avoid using the RTS/CTS mechanism for a certain 100 percent of the packets and use RTS/CTS mechanism for the rest (1) 100 percentage can be tuned to achieve best performance. Moreover the smaller percent packets should be transmitted using basic schemes without the RTS/CTS protection because the collision probability is less for the small sized packets.

3.12 CSMA/CA (used in IEEE 802.11/WiFi WLANs)

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60 GHz frequency bands.

They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997 and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the market place, each revision tends to become its own standard.

802.11 technology has its origins in a 1985 ruling by the U.S. Federal Communications Commission that released the ISM band for unlicensed use.

Wi-Fi, also spelled Wifi or WiFi, is a popular technology that allows an electronic device to exchange data or connect to the internet wirelessly using radio waves. The name is a trademark name, and was stated to be a play on the audiophile term Wi-Fi. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards". However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN".

3.13 IEEE 802.11 RTS/CTS Exchange

CSMA/CA can optionally be supplemented by the exchange of a Request to Send (RTS) packet sent by the sender S, and a Clear to Send (CTS) packet sent by the intended receiver R. Thus alerting all nodes within range of the sender, receiver or both, to not transmit for the duration of the main transmission. This is known as the IEEE 802.11 RTS/CTS exchange. Implementation of RTS/CTS helps to partially solve the hidden node problem that is often found in wireless networking.

Transmission:

If the medium was identified as being clear or the node received a CTS to explicitly indicate it can send, it sends the frame in its entirety. Unlike CSMA/CD, it is very challenging for a wireless node to listen at the same time as it transmits (its transmission will dwarf any attempt to listen). Continuing the wireless example, the node awaits receipt of an acknowledgement packet from the Access Point to indicate the packet was received and check summed correctly. If such acknowledgement does not arrive after a

timely manner, it assumes the packet collided with some other transmission, causing the node to enter a period of binary exponential backoff prior to attempting to re-transmit.

3.14 RTS/CTS HANDSHAKE with ACK

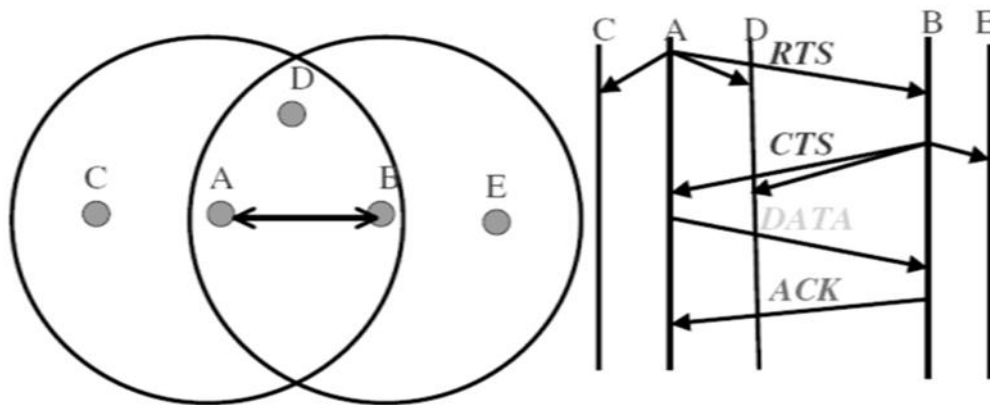


Figure 3.5: RTS/CTS HANDSHAKE with ACK

IEEE 802.11 RTS/CTS mechanism helps to solve this problem only if the nodes are synchronized. When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an exposed node and is permitted to transmit to other neighboring nodes [9]. If the nodes are not synchronized, the problem may occur that the sender will not hear the CTS or the ACK during the transmission of data of the second sender figure 3.5.

- A is the source which is in the range of B, D and C.
- B is the destination which is in the range of A, D and E.
- B sends ACK after receiving one data packet.
- Improves link reliability using ACK Figure: 3.5.

3.15 IEEE 802.11 RTS/CTS

RTS/CTS (Request to Send / Clear to Send) is the optional mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem. Originally the protocol fixed the exposed node problem as well, but modern RTS/CTS includes ACKs and does not solve the exposed node problem.

IEEE 802.11 RTS/CTS mechanism

IEEE 802.11 RTS/CTS mechanism could help solve exposed node problem as well, only if the nodes are synchronized and packet sizes and data rates are the same for both the transmitting nodes. When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an exposed node and is permitted to transmit to other neighboring nodes. [1] If the nodes are not synchronized (or if the packet sizes are different or the data rates are different) the problem may occur that the exposed node will not hear the CTS or the ACK during the transmission of data of its neighbor.

3.16 The IEEE 802.11 standard

The IEEE 802.11 standard was approved in 1997 and it defines the physical layer options for wireless transmission and MAC layer protocol. The IEEE 802.11 standard defines the protocol for two types of networks: Ad-hoc networks and client/server networks. An Ad-hoc network is a simple network where communications are established between multiple stations in a given coverage area without the use of an access point or server. All the nodes are assumed to be peers with no master station. The client/server network uses an access point that controls the allocation of transmit time for all stations and allows mobile stations to roam from cell to cell. The access point is used to handle traffic from the mobile radio to the wired or wireless backbone of the client/server network. [10]

The following figure 3.3 shows the basic topology of an 802.11 network. A Basic Service Set (BSS) consists of two or more wireless nodes, or stations (STAs), which have recognized each other and have established communications. In most instances, the BSS contains an Access Point (AP). The main function of an AP is to form a bridge between wireless and wired LANs. The AP is analogous to a base station used in cellular phone networks. IEEE 802.11 provides for two variations for the physical layer. These include two Radio Frequency (RF) technologies namely Direct Sequence Spread Spectrum (DSSS), and Frequency Hopped Spread Spectrum (FHSS). Both the DSSS and FHSS work in the 2.4 GHz of Industrial, Scientific and Medical (ISM) band. This was chosen because you don't need a license from the Federal Communications Committee (FCC) to operate on it. With direct sequence spread spectrum the transmission signal is spread over an allowed band and a random binary string is used to modulate the transmitted signal.

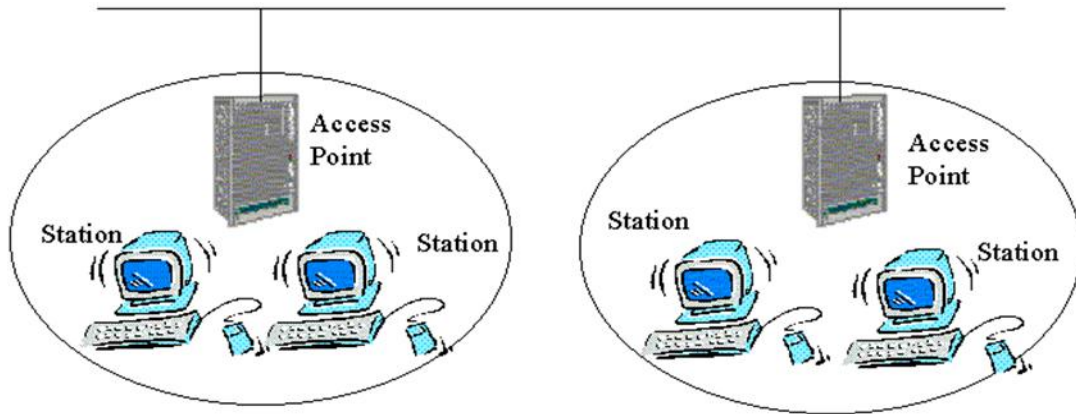


Figure 3.6: IEEE 802.11 standard's network topology.

This random string is called the spreading code. The data bits are mapped to into a pattern of "chips" and mapped back into a bit at the destination. The number of chips that represent a bit is the spreading ratio. The higher the spreading ratio, the more the signal is resistant to interference. Recovery is faster in DSSS systems because of the ability to spread the signal over a wider band. The DSSS system provides a wireless LAN with both a 1 Mbps and a 2 Mbps data payload communication capability. According to the FCC regulations, the DSSS system shall provide a processing gain of at least 10 dB. The DSSS system uses baseband modulations of Differential Binary Phase Shift Keying (DBPSK) and Differential Quadrature Phase Shift Keying (DQPSK) to provide the 1 Mbps and 2 Mbps respectively.

Recently, the IEEE 802.11 Working Group came up with a new set of standards for high speed Wireless Local Area Networks (WLAN). The IEEE 802.11 standard allows a maximum speed of 2 Mbps. The new standards viz., IEEE 802.11a and IEEE 802.11b allows speeds upto 54 Mbps. The modulation scheme used in IEEE 802.11 is normally Binary Phase Shift Keying (BPSK) or Quadrature Phase Shift Keying (QPSK). They are sufficient in 1 and 2 Mbps systems, but they do not meet the demands of higher data rate transmission schemes. To achieve the higher speeds, different modulation techniques should be implemented. [7]

3.17 Frame Format of IEEE 802.11 RTS/CTS

The RTS frame contains five fields, which are: 1.Frame Control, 2.Duration, 3.RA (Receiver Address), 4.TA (Transmitter Address) and 5.FCS.

The CTS frame contains four fields, which are: 1.Frame Control, 2.Duration, 3.RA (Receiver Address) and 4.FCS.

The ACK frame contains four fields, which are: 1.Frame Control, 2.Duration, 3.RA (Receiver Address) and 4.FCS.

RA - Receiver Address indicating the MAC Address of the station that shall receive frame.

TA - Transmitter Address indicating the MAC address of the station which has transmitted frame.

FCS - Frame Check Sequence.

This protocol was designed under the assumption that all nodes have the same transmission ranges, and does not solve the hidden terminal problem. The RTS/CTS frames can cause a new problem called the exposed terminal problem in which a wireless node that is nearby, but is associated with another access point overhears the exchange and then is signaled to back-off and cease transmitting for the time specified in the RTS.

RTS/CTS is an additional method to implement virtual carrier sensing in Carrier sense multiple access with collision avoidance (CSMA/CA). By default, 802.11 relies on physical carrier sensing only which is known to suffer from the hidden node problem.

RTS/CTS packet size threshold is 0–2347 octets. Typically, sending RTS/CTS frames does not occur unless the packet size exceeds this threshold. If the packet size that the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. Otherwise, the data frame gets sent immediately.

IEEE 802.11 implementation

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997 and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version

of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the market place, each revision tends to become its own standard.

3.18 RTS/CTS with Three Way Handshaking Protocol

MACA is a 3-way handshake (RTS/CTS/DATA) protocol and “was inspired by the CSMA/CA method (used by the Apple Local talk network for somewhat different reasons)”[9]. It can be described as follows. Still use figure 3.7 as an example. Before A sends out the data frame to B, it transmits a Request-To-Send (RTS) to B. Upon correctly receiving the RTS, B replies a Clear-To-Send (CTS) frame. After A receives the CTS, it starts the data frame transmission. During this procedure, stations that overhear the RTS frame will defer all transmissions long enough for A to receive the CTS. While stations (including C) that hear the CTS will keep quiet (because they are in B’s range, so their transmission will corrupt the frames sent from A to B).

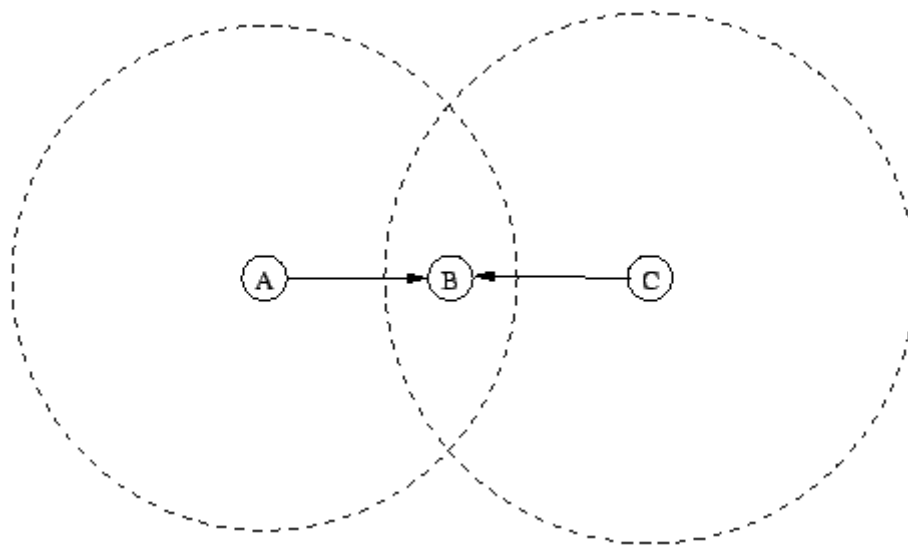


Figure 3.7: Hidden Station Problem

Using such a protocol, the hidden station problem is resolved with the help of RTS/CTS handshake, i.e., C will not interrupt the transmission from A to B even though it cannot sense the ongoing transmission.

In [3], the “exposed station” problem that is closely related to the hidden station problem is discussed. As shown in Figure 3.8, the transmission from C to D has been going on when B wants to send data to A. Under such a situation, potential concurrent transmission

(B to A) is prohibited because B is exposed to the ongoing C to D transmission. Although the exposed station problem does not cause collision, it degrades the network throughput. Meanwhile, the exposed station problem is also addressed to some extent. Consider the scenario described at the beginning of this section. Assume that the C to D transmission used RTS/CTS/DATA handshake, B must have heard C's RTS, but B could not hear D's CTS. According to MACA, B only has to wait long enough for C to finish receiving the CTS from D. After that, B can go ahead to initiate the transmission to A instead of wait until C to D data transmission completes.

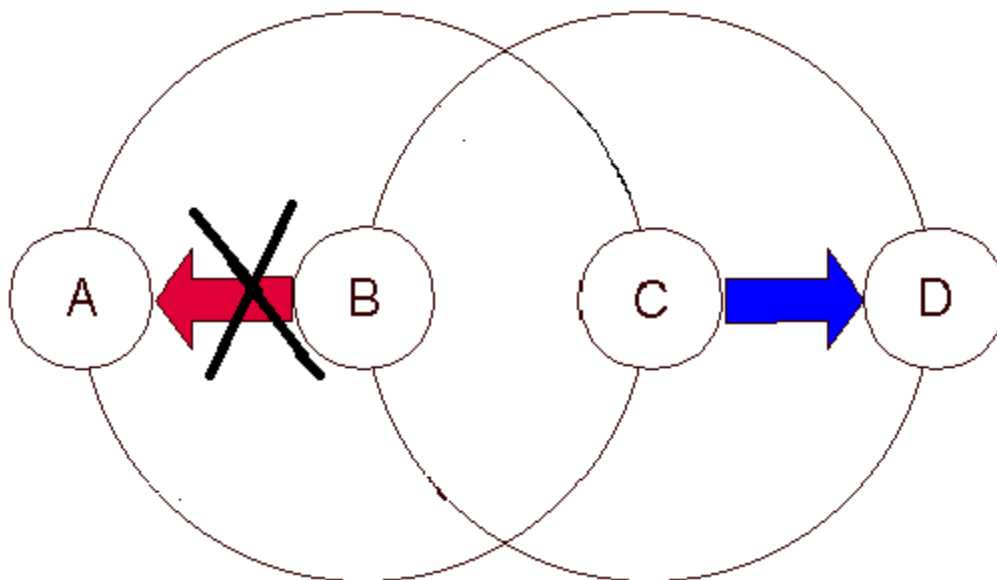


Figure 3.8: Exposed Station Problem

3.19 Three Way Handshake

A three-way-handshake is a method used in a TCP/IP network to create a connection between a local host/client and server. Three Way Handshake process complete in three steps. They are:

RTS(Request To Send),CTS(Clear To Send) and Data(message or Information or Audio Or Video).

Establishing a normal TCP connection requires three separate steps:

1. The first host (Alice) sends the second host (Bob) a "synchronize" (SYN) message with its own sequence number x , which Bob receives.
2. Bob replies with a synchronize-acknowledgment (SYN-ACK) message with its own sequence number y and acknowledgement number $x + 1$, which Alice receives.
3. Alice replies with an acknowledgment message with acknowledgement number $y + 1$, which Bob receives and to which he doesn't need to reply.

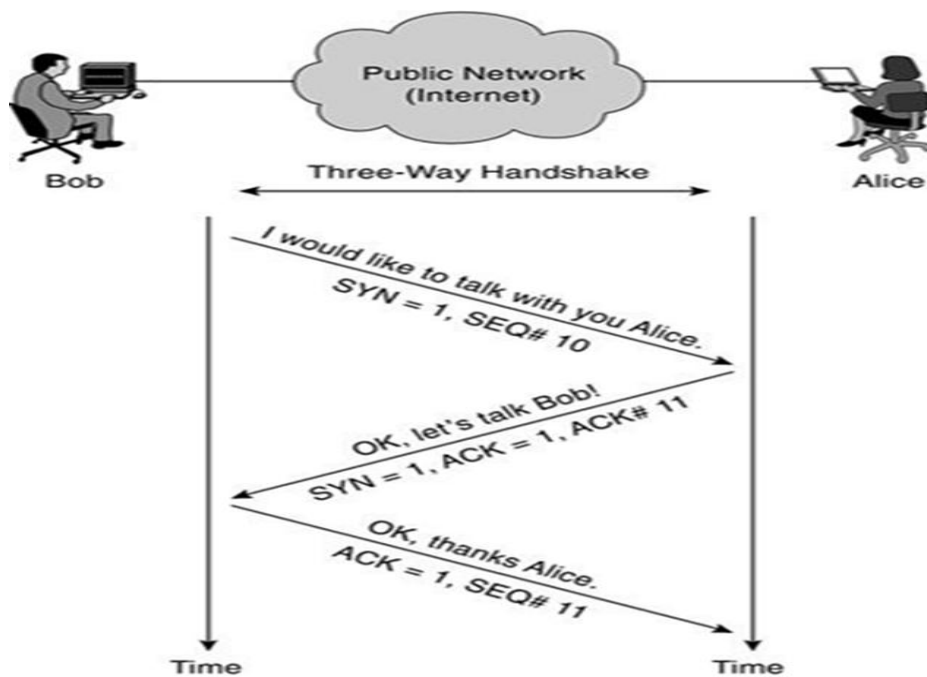


Figure 3.9: Establish Three Way Handshaking

In this setup, the synchronize messages act as service requests from one server to the other, while the acknowledgement messages return to the requesting server to let it know the message was received. One of the most important factors of three-way handshake is that, in order to exchange the starting sequence number the two sides plan to use, the client first sends a segment with its own initial sequence number x , then the server responds by sending a segment with its own sequence number y and the acknowledgement number $x + 1$, and finally the client responds by sending a segment with acknowledgement number $y + 1$. The reason for the client and server not using the default sequence number such as 0 for establishing connection is to protect against two

incarnations of the same connection reusing the same sequence number too soon, which means a segment from an earlier incarnation of a connection might interfere with a later incarnation of the connection.

3.20 Three Way Handshaking Protocol

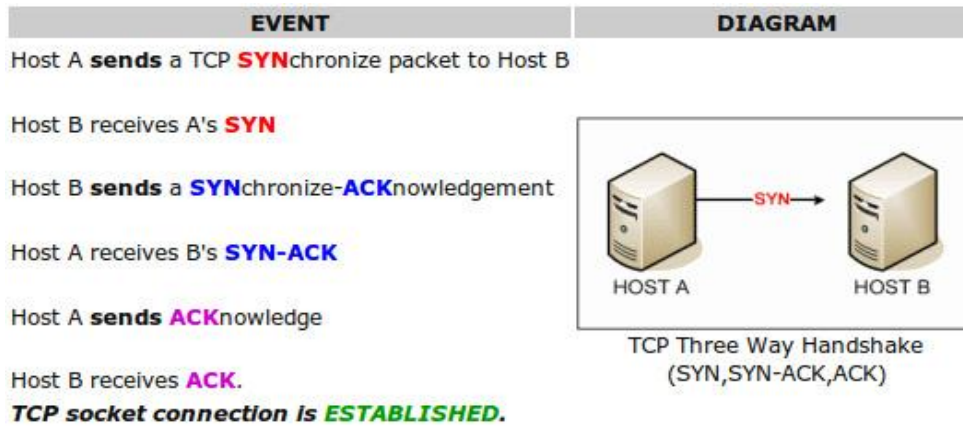
Three Way Handshaking Protocol is TCP/IP protocol. The TCP three-way handshake in Transmission Control Protocol (also called the TCP-handshake; three message handshake and or SYN-SYN-ACK) is the method used by TCP set up a TCP/IP connection over an Internet Protocol based network. TCP is a connection oriented Transport Layer protocol. As internet architecture is best effort, packet losses occur very often. But application layer wants reliability. So, this has to be done by TCP. Applications run only on the end host. So some process to process communication facilities should be provided and TCP does this. At each end host TCP takes care of reordering of packets, packet loss, flow control and many other things. To do all these things, TCP establishes a point-to-point connection between two hosts. For reliable connection establishment it uses three way handshaking, i.e. three specialized packets are transferred between the two hosts to agree on the connection. TCP's three way handshaking technique is often referred to as "SYN-SYN-ACK" (or more accurately SYN, SYN-ACK, ACK) because there are three messages transmitted by TCP to negotiate and start a TCP session between two computers. The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of the network TCP socket connection before transmitting data such as SSH and HTTP web browser requests.

This 3-way handshake process is also designed so that both ends can initiate and negotiate separate TCP socket connections at the same time. Being able to negotiate multiple TCP socket connections in both directions at the same time allows a single physical network interface, such as Ethernet, to be multiplexed to transfer multiple streams of TCP data simultaneously. [10]

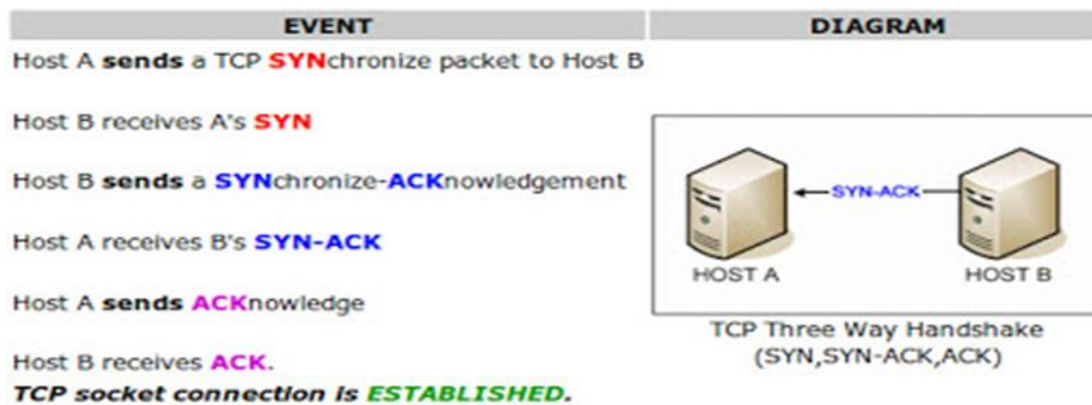
3.21 TCP Three Way Handshake

The three-way handshake is done in the following process:-

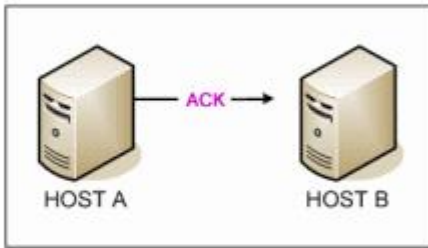
1. The client sends a SYN packet to the server indicating that it wants to set a TCP connection. It also sends ISN (Initial Sequence Number). Here ISN is x.

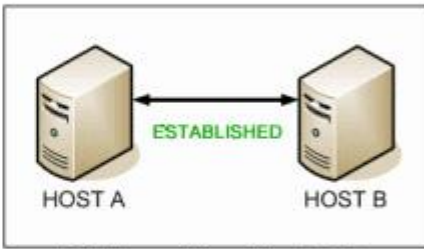


2. If the server is 'alive' and listening on the requested port and can accept an incoming connection, it replies with its own SYN + ACK packet. It sends its own ISN (Initial Sequence Number)(for this connection, y) and acknowledges the clients request by sending back client's ISN + 1 sequence number ($x + 1$).



3. Finally, after receiving the server's SYN + ACK response, the client sends back an ACK packet with a sequence number of server's ISN + 1 ($y + 1$).

EVENT	DIAGRAM
Host A sends a TCP SYN chronize packet to Host B	
Host B receives A's SYN	
Host B sends a SYN chronize- ACK nowledgement	 <p data-bbox="922 573 1246 636">TCP Three Way Handshake (SYN,SYN-ACK,ACK)</p>
Host A receives B's SYN-ACK	
Host A sends ACK nowledge	
Host B receives ACK .	
TCP socket connection is ESTABLISHED.	

EVENT	DIAGRAM
Host A sends a TCP SYN chronize packet to Host B	
Host B receives A's SYN	
Host B sends a SYN chronize- ACK nowledgement	 <p data-bbox="874 1218 1195 1281">TCP Three Way Handshake (SYN,SYN-ACK,ACK)</p>
Host A receives B's SYN-ACK	
Host A sends ACK nowledge	
Host B receives ACK .	
TCP socket connection is ESTABLISHED.	



3.22 TCP Segment Structure

The TCP segment consist of a header fields and data field.

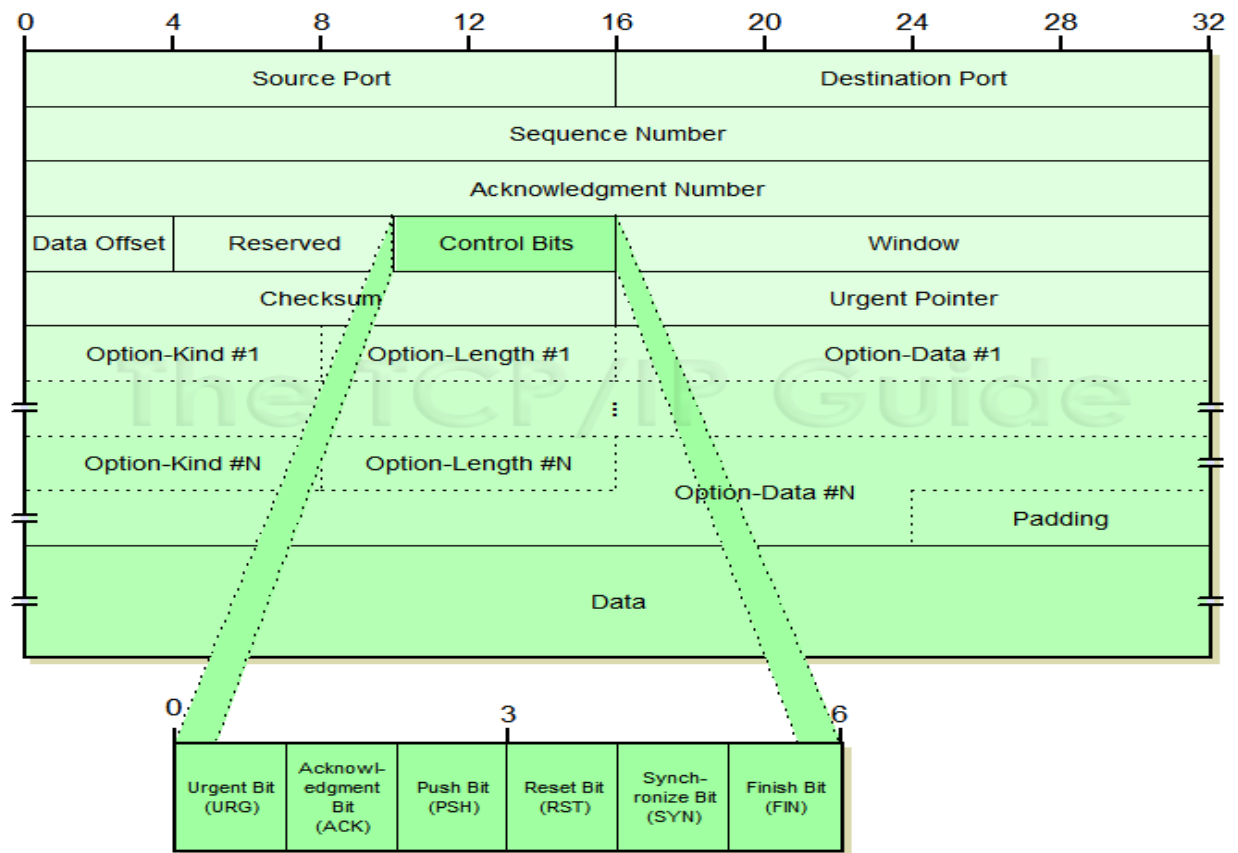


Figure 3.10: TCP Segment Structure

In the header field, there is a flag field contains 6 bits. The ACK bit is used to indicate that the value carried in the acknowledgement field is valid. The RST, SYN and FIN bits are used for connection setup and teardown. PUSH bit indicates that data should pass to the upper layer immediately. Finally, the URG bit is used to indicate some data has marked urgent by the sender. [10] The RST and SYN bits play import role in connection setup.

Chapter: 04

Validation by Simulation

4.1 Network Simulator 2

Network simulation software enable us to predict behavior of a large-scale and complex network system such as Internet at low cost under different configurations of interest and over long period. Many network simulators, such as NS2, Openet, Qualnet are widely available. We have used NS2 for this thesis. NS2 is a discrete event simulator written in C++, with an OTcl interpreter shell as the user interface that allows the input model files (Tcl scripts) to be executed. Most network elements in NS2 simulator are developed as classes, in object-oriented fashion. The simulator supports a class hierarchy in C++, and a very similar class hierarchy in OTcl. The root of this class hierarchy is the TclObject in OTcl. Users create new simulator objects through the OTcl interpreter, and then these objects are mirrored by corresponding objects in the class hierarchy in C++. NS2 provides substantial support for simulation of TCP, routing algorithms, queuing algorithms, and multicast protocols over wired and wireless (local and satellite) networks, etc. [11] It is freely distributed, and all source code is available. Developing new networking protocols and creating simulation scripts are complex tasks, which requires understanding of the NS2 class hierarchy, C++, and Tcl programming. However, in this thesis, we have designed and ran simulations in Tcl scripts using the simulator objects without changing NS2 core components such as class hierarchy, event schedulers, and other network building blocks. The only change has been in the codes of IEEE 802.11 mac layer and it's associated timers.

4.2 Experimental Setup

First we installed NS2 software. Then designed the simulation of TCP Three Way Handshaking protocol with hidden nodes.

4.3 Working Procedure:

NS2 software, here we used terminal to create a .tcl folder. We wrote the coding that .tcl folder where we used ten nodes and run. When it was run successfully, then it showed network simulation animator. We also saw ten nodes in simulation topology figure 4.1.

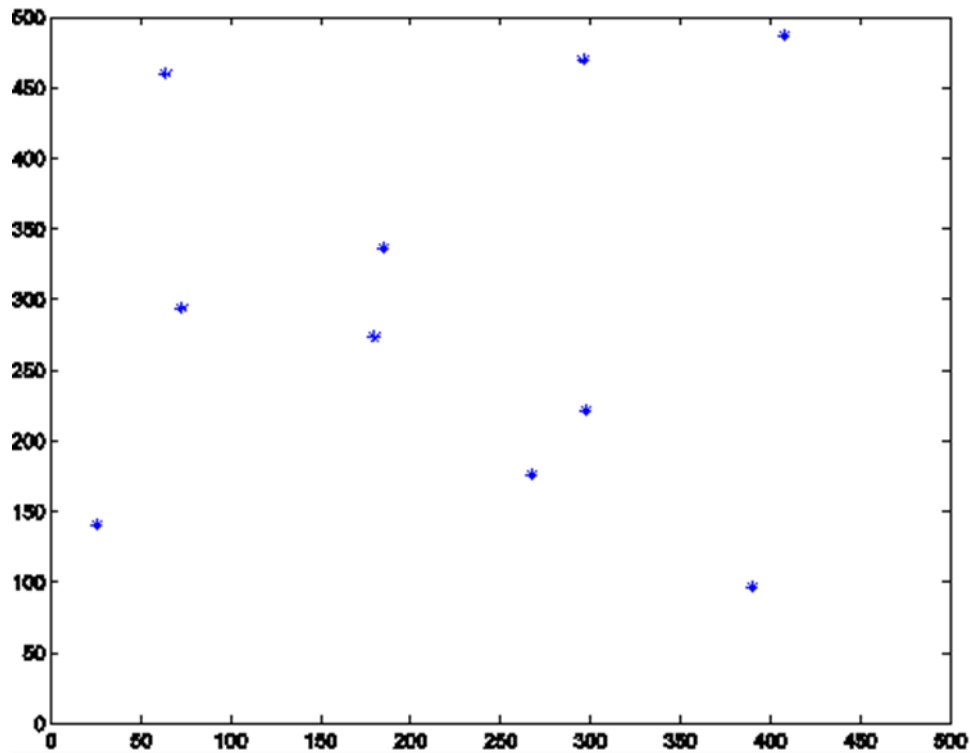


Figure 4.1: Simulation Topology

We also used xgraph to see the graph of line connectivity of ten nodes. The ten nodes connected internal to the all nodes in figure 4.2.

RTS ON in node 1 to node 3 the color of line is red. RTS OFF in node 1 to node 3 the color of line is blue. Similarly RTS ON in node 7 to node 5 the color of line is sky. RTS OFF in node 7 to node 5 the color of line is green. All are shown in figure 4.3.

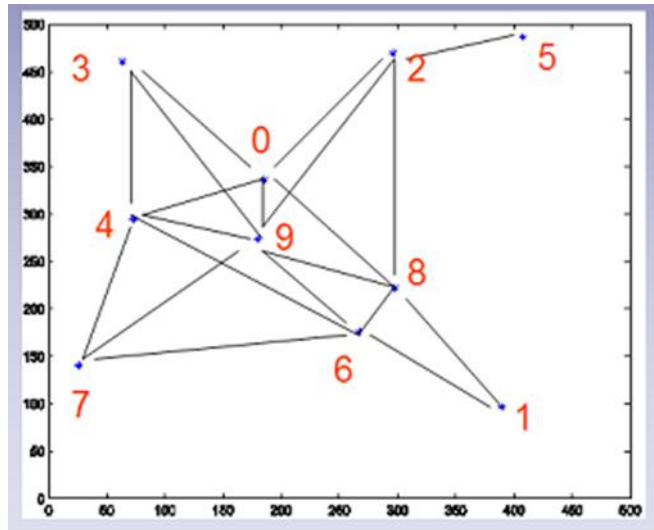


Figure 4.2: Line Connectivity Graph

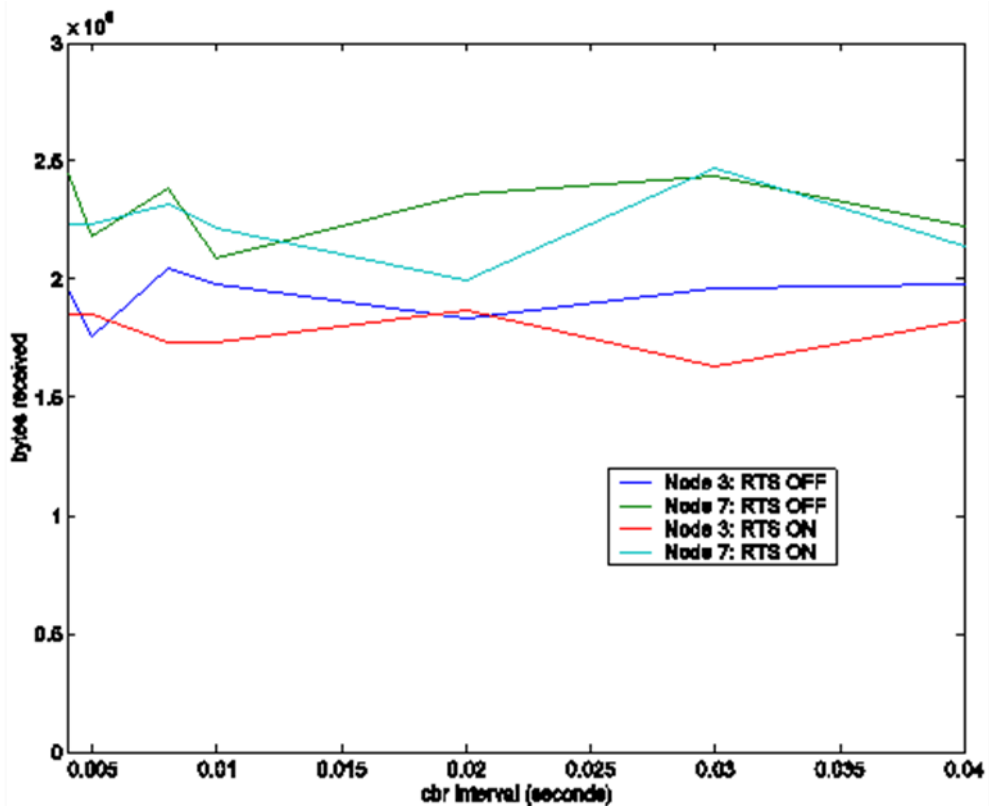


Figure 4.3: Result

4.4 Simulation Parameters:

Data transmission parameters are given below in table 4.1 between two nodes. When RTS ON Between two nodes then the data rate is 1 Mbps, IFQ (Inter Frame Queue) Length is 50, Routing Protocol is DSDV (Destination Sequenced Distance Vector). Data transmission of two nodes packet size is 1000 Bytes, Packet rate is 25-200 Per second, transmission range is 250m, test duration is 150sec.

Data rate	1 Mbps
IFQ Length	50
Routing Protocol	DSDV
Packet size	1000 Bytes
Packet rate	25-200 Per second
Transmission Range	250 m
Test duration	150 sec

Table 4.1: Simulation parameter of data transmission

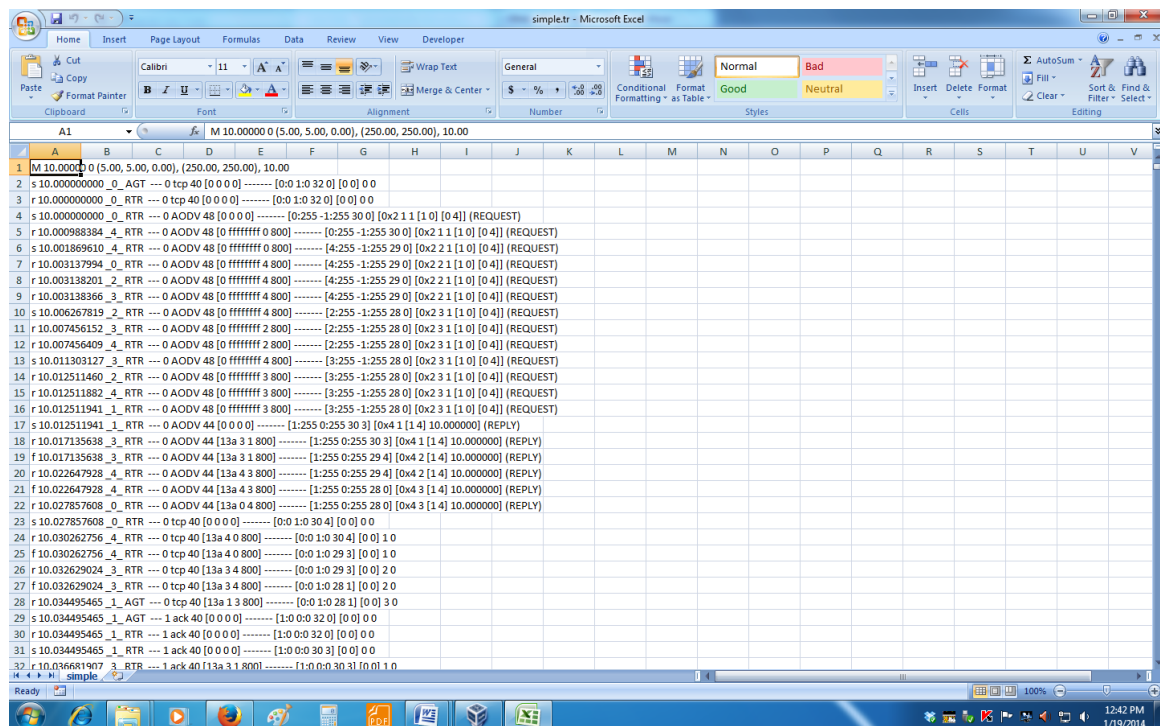


Figure 4.4: Data packet analysis.

In the experiment it is seen that total 57586 packets has been generated and among them 19493 packets has been sent and 63 packets has been dropped for MACA protocol. For CSMA/CA total 56597 packets has been generated and among them 19423 packets has been sent and 96 packets has been dropped.

Protocol	Total no. packet	packet sent	Packet dropped	Error
CSMA/CA	56597	19423	96	0.49%
MACA	57586	19493	63	0.32%

Table 4.2: Data comparison of packet analysis.

Chapter: 05

CONCLUSION

5.1 Conclusion:

In this paper, we characterized the performance of CSMA/CA adapted MAC in widely deployed IEEE 802.11 WLANs. Along with the discussion on modification approaches that best represent the possible ways that could be carried out to upgrade conventional CSMA/CA into hidden node moving aware CSMA/CA, we provided their detail performance analysis, based on the analytical modeling and derived expressions, in terms of Three Way Handshaking protocol. Thus, on the one hand, after presenting the importance analysis MAC protocol, we presented the discussion on modification approaches and the analytical model to understand their performance, while on the other hand, we also showed the moving hidden node using Three Way Handshaking protocol is expressed NS2 because of the effects of indispensable overhead associated. Hidden node problem can be solved by many means but each solution is for particular scenario. Using different techniques like Increase Transmitting Power From the Nodes, Use Omni-directional antennas, Remove obstacles, Move the nodes, Use protocol enhancement software, Use antenna diversity, Wireless Central Coordinated Protocol etcetera would increase the performance of ad-hoc networks a lot.

5.2Future Work:

For this way when hidden nodes are moved, then huge energy is lost and time is wasted. So, we will try to better solution in future that will decrease energy and time and highly motivated the carrier sense multiple access with collision avoidance

REFERENCES:

- [1] http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance
- [2] Data Communication and Networking, Third Edition, Behrouz A. Forouzan, DeAnza College with Sophia Chung Fegan [Chapter:13]
- [3] Pommer, Hermann, "Roaming zwischen Wireless Local Area Networks", VDM Verlag, Saarbrücken 2008, ISBN 978-3-8364-8708-5 C. Rama Krishna, "STTP on Wireless Communication", 2009.
- [4] D. Chen, J. Deng, P. K. Varshney, "Protecting wireless networks against a denial of service attack based on virtual jamming", 9th ACM Annual International Conference on Mobile Computing and Networking (MobiCom) Poster, 2003.
- [5] P. Karn, "MACA—a new channel access method for packet radio", 9th Computer Networking Conference on ARRL/CRRL Amateur Radio, pp. 134–140, 1990.
- [6] S. Ray, J. B. Carruthers, and D. Starobinski, "RTS/CTS-induced congestion in ad hoc wireless LANs", WCNC, 2003.
- [7] http://en.wikipedia.org/wiki/IEEE_802.11_RTS/CTS
- [8] J. Bellardo, S. Savage, "802.11 denial of service attacks: Real vulnerabilities and practical solutions", Proc-Security Symposium, 2003.
- [9] Ashikur Rahman, Pawel Gburzynski, "Hidden Problems with the Hidden Node Problem", 23rd Biennial Symposium on Communications
- [10] <http://www.eunice-forum.org/eunice99/027.pdf>
- [11] http://www.hamilton.ie/publications/Thesis_tianji.pdf