Performance Analysis of CSMA/CA in Wireless Local Area Network

Muhammad Younus	A.K.M Fazlul Haque	Md. Zahirul Islam
Daffodil International University	Daffodil International University	Daffodil International University
102, Sukrabad, Mirpur Road	102, Sukrabad, Mirpur Road	102, Sukrabad, Mirpur Road
Dhanmondi, Dhaka	Dhanmondi, Dhaka	Dhanmondi, Dhaka
Bangladesh	Bangladesh	Bangladesh

ABSTRACT

With the rapid advance of mobile computing, high speed Wireless Local Area Networks (LAN) attracts a lot of research interests in recent years. A new international stander IEEE 802.11 on wireless LAN has been established. Its physical transmission is realized by either spread spectrum communication or non-directive infrared. The medium access control of IEEE 802.11 is using carrier sense multiple access with collision avoidance (CSMA/CA) as the basic level access. Continuing from the study of, we shall analyze IEEE 802.11 CSMA/CA performance with or without RTS/CTS in this paper. We have improved the simulation by including RTS/CTS exchanges, which is part of the CSMA/CA protocol. Using this methodology, we hoped to increase the number of successful transmissions and decrease the number of collisions within the WLAN. This particular aspect of the simulation is demonstrated in the Analysis section of this work. Additionally, the simulation makes sure that once an RTS/CTS handshake is completed; all other nodes not included in the data exchange remain silent. This is done to prevent nodes from getting into a continuous cycle of RTS/CTS exchanges.

General Terms

Wireless Local Area Network, CSMA/CA

Keywords

IEEE 802.11, CTS/RTS

1. INTRODUCTION

The world of today has become quite fast and reliable mainly because of the wireless communication. In our work we have studied on CSMA/CA and its performance analysis in wireless local area network i.e. WLAN. We have simulated the code in MATLAB and get graphs by varying different parameters. By providing enough reasons and explanation finally we would like to comment on the performance of the CSMA/CA protocol and discuss the future aspect of it.

With the simulation graphs and explanations, checking the respected theories we can conclude that using RTS/CTS in CSMA/CA protocol is efficient. Because in the WLAN we would like to get as much higher the transmission to get as possible and lower the collision among the different nodes. We can see the clear evidence that we have given from our simulation of the CSMA/CA protocol that without using RTS/CTS in the protocol gives the much poor result in the transmission and collision. But if we use RTS/CTS the transmission increases as well as the collision decreases. And in the increased number of nodes the performances of CSMA/CA protocol also increases for using the RTS/CTS

condition. So the assumption of using RTS/CTS in the CSMA/CA protocol in every condition provides much efficiency is proven here.

2. OVERVIEW OF WLAN

All Wireless LAN is a member of the IEEE 802 family of specifications for Local Area Networks which allows computers to get connected to a network through wireless[1]. And because of wireless is a shared medium, everything that is transmitted or received over a wireless network can be intercepted.

Prot ocol	Rele ase date	Op. Frequ ency	Throug hput (Typ)	Dat a Rat e (M ax)	Modul ation Techni que	Ran ge (Rad ius Indo or)	Rang e (Radi us Outd oor)
Lega cy	1997	2.4GH z	0.9 Mbps	2 Mb ps		~20 m	~100 m
802.1 1a	1999	5 GHz	23 Mbps	54 Mb ps	OFDM	~35 m	~120 m
802.1 1b	1999	2.4GH z	4.3 Mbps	11 Mb ps	DSSS	~38 m	~140 m
802.1 1g	2003	2.4GH z	19Mbps	54 Mb ps	OFDM	~38 m	~140 m
802.1 1n	June - 2009	2.4GH z 5 GHz	74Mbps	248 Mb ps		~70 m	~250 m
802.1 1y	June - 2008	3.7 GHz	23Mbps	54 Mb ps		~50 m	~5000 m

Table 1**:** Characteristics of different version of wireless network protocols[1].

A survey had found that about 70% of wireless network have no security at all. Among them IEEE 802.11b [2] is the most popular and widely used protocol in Wireless area. So, we choose 802.11b and it's really important to ensure security in WLAN.

There are two basic modes of operation specified in the standard. The most commonly used mode is the infrastructure mode. The infrastructure mode allows for either one of the entities to be an access point. In ad-hoc mode all entities are considered clients. Ad-hoc mode may also be referred to as independent mode. Stations in adhoc mode participate in an adhoc network, likewise if they are in infrastructure mode

they participate in an infrastructure network. Interface of a client or access point contains a radio and an antenna. To avoid interference and allow networks to operate in the same locations, IEEE 802.11 specifies groups of frequencies that may be utilized by a network.

Wireless LANs undoubtedly provides higher productivity and cost savings. In light of this, many organizations are beginning to deploy wireless LAN technologies not only for Cost savings, but also for convenience and flexibility of use. But the fundamental question plaguing the industry today is if wireless networks can be deployed securely without compromising organization's assets - information. This study was undertaken to find out if wireless networks are inherently insecure thereby limiting enterprise deployment. If yes, what are the known holes, and can they be fixed? The following are the contributions to knowledge this work has made through exhaustive and broad literature study[14]:

1. This study has shown that wireless LANs is prone to many different kinds of attacks. Attempt to secure wireless LANs, suitable for enterprise deployment, initiated a move from weak WEP to more robust WPA2.

2. This work also showed that the most effective security solution for Wireless LANs involves a combination of security technologies.

3. It demonstrated that a thorough vulnerability assessment and risk analysis is essential for development of effective security policy and determination of appropriate security measures, or combination of measures that are most effective.

4 It also showed that countermeasures and best practices - like personal firewalls, antivirus, intrusion detection systems etc. - typically used to defend Internet connected

Clients are generally recommended for WLAN clients as well.

5. On-going monitoring and periodic testing are necessary to verify that a deployed WLAN meets defined objectives.

3. CARRIER SENSE MULTIPLE ACCESS/COLLISION AVOIDANCE (CSMA/CA)

In Wireless LANs CSMA/CA is core concept in communicating wirelessly. In any shared medium accessing the medium without collision is important part. Its like not talking all at a time, so that remaining people should understood the other's talk. To know about CSMA/CA we have to know CSMA.

Carrier Sense Multiple Access (CSMA) is one of most popular random access protocols in practice, which we see in most of wireless textbooks. The key features of CSMA is that each link with a pair of transmitter and receiver senses the medium and transmits a packet only if the medium is sensed idle. Due to its simple and distributed nature, it has been regarded as one of the most practical MAC protocols. in wireless networks, e.g., CSMA is a basic medium access algorithm in IEEE 802.11. Thus, there exists a vast array of research results on CSMA in terms of its analysis under various settings and its applications to practical systems.

CSMA maintain a rule on a network that one point can transmit data, otherwise it may will loss of data/frames. CSMA active at the time when a point wants to send data or signal on a network. It always checks or listen for network traffic before transmitting a signal or data frame, if it find any other transmission is in process then it will pause its own

process up to the previous process completed. However, if multiple devices access it simultaneously and a collision occurs, they both have to wait for a specific time before reinitiating the transmission process [7].

3.1 Flow chart of CSMA/CA

In CSMA/CA, when a point or node receives a packet that is to be sent, it checks for free time period of a channel by which the node can sent the packet. In CSMA, a node or device have to wait for a time interval if it find a busy or transferring process on the network. The time period is known as back-off factor. Back-off factor is measure with back-off counter. When the transmitting channel is clear, back-off counter reaches to zero and the device starts to send data/packet. And when the transmitting channel is not clear but back-off counter is reaches to zero it means that the process is repeated from the sensing again the channel for random time.[10] [11]
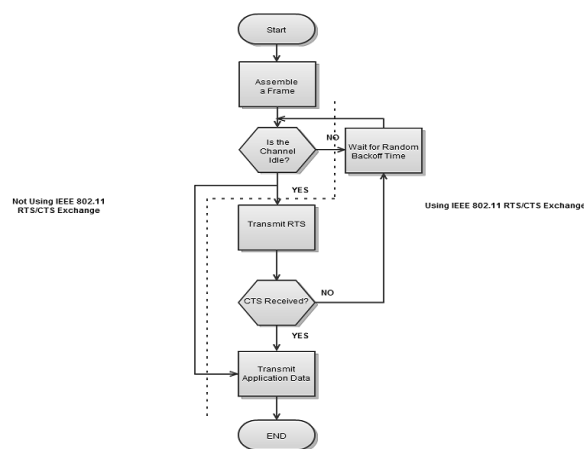

Fig 1: Flow chart of CSMA/CA[11]

3.2 Basic operation of CSMA/CA

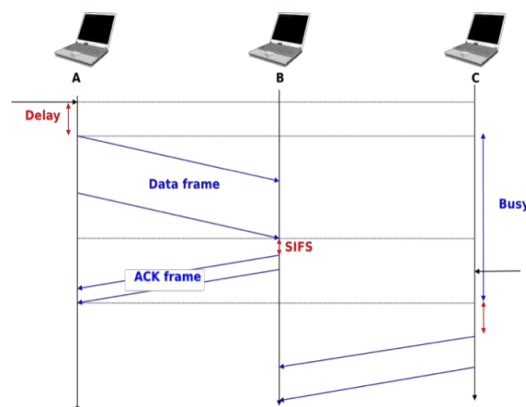Now I discuss the basic operation of CSMA/CA device. This figure is the basic operation of CSMA/CA.

Fig 2: Basic operation of CSMA/CA [9].

Before transmitting, host A verifies that the channel is empty for a long enough period. Then, its sends its data frame[14]. After checking the validity of the received frame, the recipient sends an acknowledgement frame after a short SIFS delay. Host C, which does not participate in the frame exchange, senses the channel to be busy at the beginning of the data frame. Host C can use this information to determine how long the channel will be busy for. Note that as SIFS<DIFS<EIFS, even a device that would starts to sense the channel

immediately after the last bit of the data frame could not decide to transmit its own frame during the transmission of the acknowledgement frame.

3.3 Collision of CSMA/CA

The main difficulty with CSMA/CA is when two or more device transmits at the same time and cause collisions. This is illustrated in the figure below, assuming a fixed timeout after the transmission of a data frame. With CSMA/CA, the timeout after the transmission of a data frame is very small, since it corresponds to the SIFS plus the time required to transmit the acknowledgement frame.
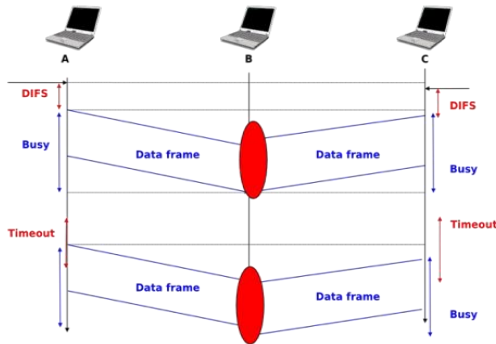
Fig 3: collision with CSMA/CA[6]

To deal with this problem, CSMA/CA relies on a back off timer[6]. This back off timer is a random delay that is chosen by each device in a range that depends on the number of retransmissions for the current frame. The range grows exponentially with the retransmissions as in CSMA/CD. The minimum range for the back off timer is where the slot Time is a parameter that depends on the underlying physical layer. Compared to CSMA/CD's exponential back off, there are two important differences to notice. First, the initial range for the back off timer is seven times larger. This is because it is impossible in CSMA/CA to detect collisions as they happen. With CSMA/CA, a collision may affect the entire frame while with CSMA/CD it can only affect the beginning of the frame. Second, a CSMA/CA device must regularly sense the transmission channel during its back off timer. If the channel becomes busy (i.e.)Because another device is transmitting), then the back off timer must be frozen until the channel becomes free again. Once the channel becomes free, the back off timer is restarted. This is in contrast with CSMA/CD where the back off is recomputed after each collision. This is illustrated in the figure below. Host A chooses a smaller back off than host C. When C senses the channel to be busy, it freezes its back off timer and only restarts it once the channel is free again. We need some system configuration in our work.[10] [11]

3.4 How to avoid collision in CSMA/CA

Do For avoiding collision in CSMA/CA, every device can reserve the operating channel for short period of time. The exchange of two control frames- Request to Send(RTS) and Clear to Send(CTS) are used to avoid the risk of collisions between different node in the network. For reserving a channel, first one device send RTS frame to intended destination device. this RTS frame contains the information about reservation period. The other devices replies by a CTS control frame which also contain information about duration of channel reservation. As the duration of the reservation has been sent in both RTS and CTS, all hosts that could collide

with either the sender or the reception of the data frame are informed of the reservation. They can compute the total duration of the transmission and defer their access to the transmission channel until then. This is illustrated in the figure below where host A reserves the transmission channel to send a data frame to host B. Host C notices the reservation and defers its transmission[4].
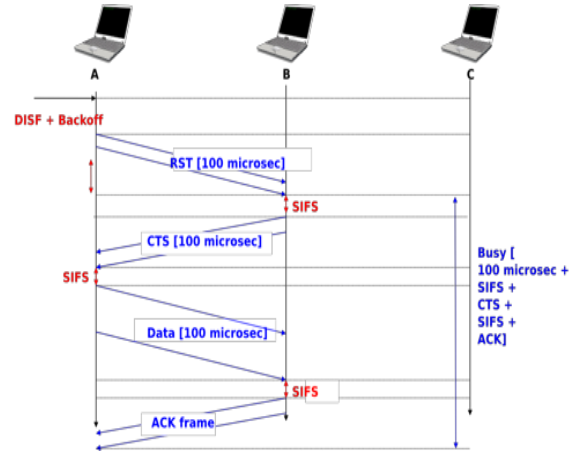

Fig 4: Avoid collision in CSMA/CA[4].

not include headers, footers or page numbers in your submission. These will be added when the publications are assembled.

4. SIMULATION AND RESULTS

To analyze the CSMA/CA protocol we have created a similar simulation environment considering the transmission of different nodes. And then we have simulated the protocol, in this simulation we have varied different variables. These variables are –

1. CSMA/CA protocol with RTS/CTS
2. CSMA/CA protocol without RTS/CTS
3. Changing the no. of nodes for both cases.

So far what we have got from the simulation are included in this point. We would like to explain the results with graphical representation. By providing enough reasons and explanation finally we would like to comment on the performance of the CSMA/CA protocol and discuss the future aspect of it.

Successful transmission when the no. of node is less or equal 5

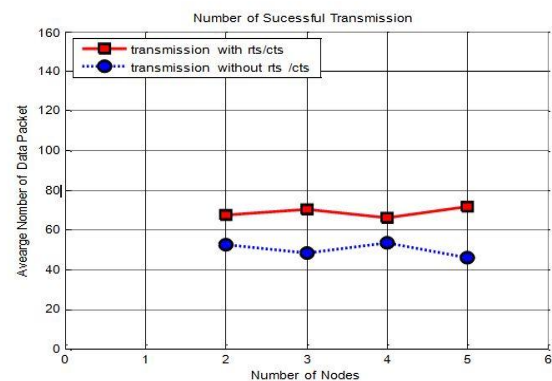First of all here is the graph of successful transmission when the no. of node is less or equal 5.

Figure 5: Successful transmissions with and without rts-cts when node number is ≤5

Simulation Data

Transmission with rts/cts	67.5	70.2	66	72
Transmission without rts/cts	52.4	48.3	53.8	46.2

Table 2: Simulation Data (transmissions) for when node number is ≤5

Here the X-axis denotes the number of nodes and Y-axis stands for average number of data packets. From the graph we can see two different color of lines. The red line represents the transmission with RTS/CTS and blue one is for transmission without RTS/CTS. This graphical representation is enough to comment that if we use RTS/CTS in CSMA/CA protocol the successful transmission is higher than the other one. Average number of data packets value is given in a table also, from which we can conclude the same.

Bar-Chart:

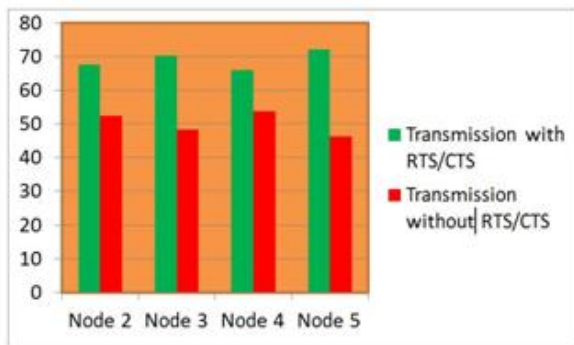For a better understanding we can use the bar chart and here it is –

Figure 6: Successful transmissions with and without rts-cts when node number is ≤5(Bar-Chart)

The green color represents the transmission with RTS/CTS and the red is for the other protocol. From here we can clearly see that the difference between this two protocol with respect to average number of data packets is much higher. And the transmission with RTS/CTS wins over the other.

Collision rate when the no. of node is less or equal 5

Though we can conclude that using RTS/CTS in CSMA/CA is better by seeing the transmission graph, we would like to see what does happen in the collision –
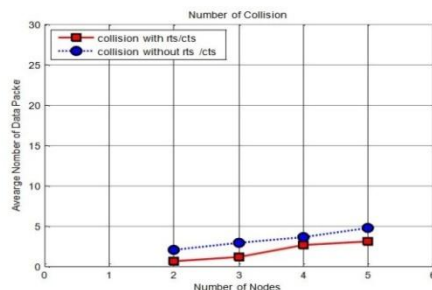

Figure 7: Collision rate with and without rts-cts when node number is ≤5

Collision with rts/cts	0.7	1.2	2.7	3.1
Collision without rts/cts	2.1	2.9	3.6	4.8

Simulation Data

Table 3: Simulation Data (collision) for when node number is ≤5

In the graph the axis's denote the same again and blue or red color indicates the same as before. If we use RTS/CTS then the collision decreases that we can see from the graph. For the number of node respected values are given also in the tabular form. If we want to see the collision difference for these two protocols with respect to individual node point this bar chart provides much more clear explanation
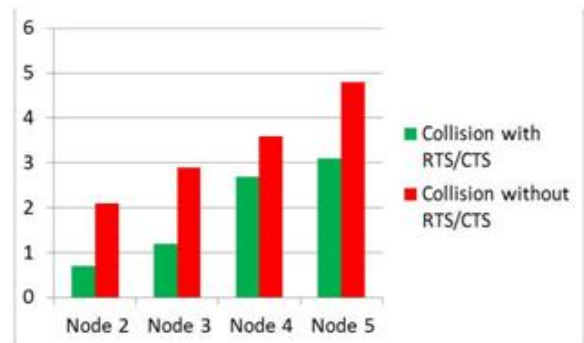
Bar-Chart

Figure 8: Collision rate with and without rts-cts when node number is ≤5(Bar-Chart)

For every single node the red one that means collision without RTS/CTS in the CSMA/CA protocol gives higher values. So in the sense of collision using RTS/CTS in the protocol provides better result since in here collision is less, so transmission would be higher.

Successful transmission when increase the number of nodes

Now we would like to increase the number of nodes and see what happens in the transmission and collision graph. First the successful transmission graph
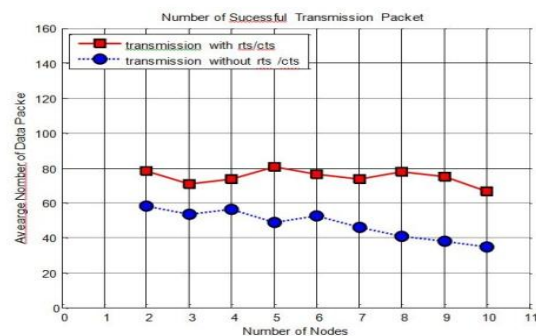

Figure 9: Successful transmissions with and without rts-cts in when node number is increasing.

Simulation Data

Transmission with rts/cts	78.5	71	73.8	80.5	76.4	73.5	78	75.2
Transmission without rts/cts	58.3	53.4	56.2	48.7	52.5	46.1	41	38.3

Table 4: Simulation Data (transmission) for when node number is increasing

Here the number of node is increased from 5 to 10. The graphical parameters are same as before. Since from the graph we can understand that the red line has higher values in the transmission process we can conclude that the RTS/CTS is better than the another protocol. With the increased number of nodes the transmission continuously decreases for without RTS/CTS but using RTS/CTS can get better packet transmission. The tabular data for successful transmission supports the same conclusion.

Bar-Chart

For a clear understanding in each of the nodes this bar chart helps to shade a brighter light
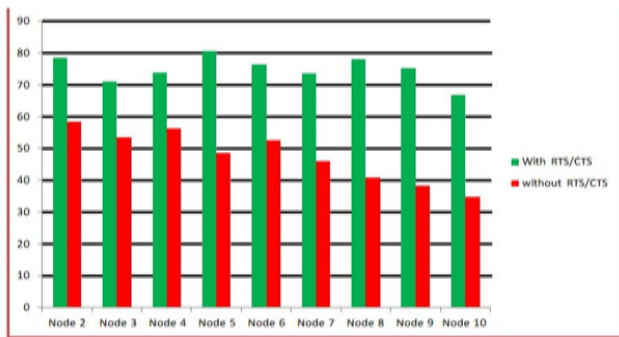

Figure 10: Successful transmissions with and without rts-cts in when node number is increasing(Bar-Chart)

Here the green one is for RTS/CTS which is higher in every node than the without RTS/CTS. The higher the better transmission, so RTS/CTS has better performance on the increased number of nodes.

Collision rate when increase the number of nodes:

If we do not use RTS/CTS in the CSMA/CA protocol for the increased number of nodes the collision would increase for each increased number of node. This graph of collision provides the same result
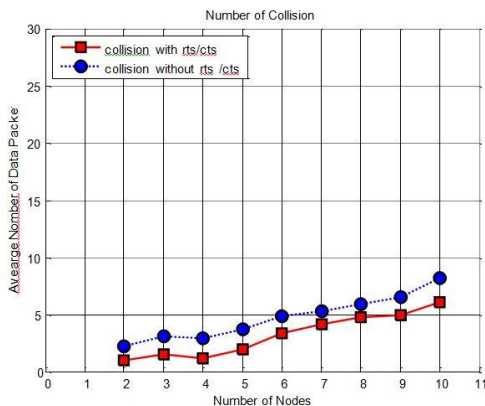

Figure 11: Collision rate with and without rts-cts in when node number is   increasing

Simulation Data

Collision with rts/cts	1	1.5	1.2	2	3.4	4.2	4.8	5	6.1
Collision without rts/cts	2.2	3.1	2.9	3.7	4.9	5.3	5.9	6.5	8.2

Table 5: Simulation Data (collision) for when node number is increasing.

Here we can clearly see that the blue line means the collision without RTS/CTS is higher than the red line means collision with RTS/CTS. If the collision is lower the better so the blue line refers that not using RTS/CTS in the CSMA/CA protocol get the worse result.

Bar-Chart

Again if we would like to get the clear picture what really happens in the each node this bar chart will help to understand
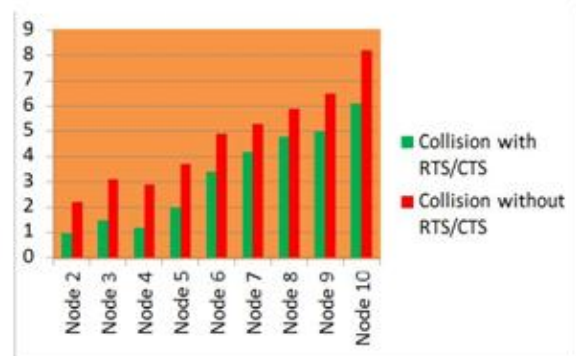

Figure 12: Collision rate with and without rts-cts in Bar-Chart when node number is increasing.

With the increased number of nodes in each node the collision without RTS/CTS is much higher than the collision with RTS/CTS. We can sum up that the higher the collision the worsen the performance, so without using RTS/CTS will provide the poor performance in the CSMA/CA protocol.

5. ANALYSIS

With the simulation graphs and explanations, checking the respected theories we can conclude that using RTS/CTS in CSMA/CA protocol is efficient. Because in the WLAN we would like to get as much higher the transmission to get as possible and lower the collision among the different nodes. We can see the clear evidence that we have given from our simulation of the CSMA/CA protocol that without using RTS/CTS in the protocol gives the much poor result in the transmission and collision. But if we use RTS/CTS the transmission increases as well as the collision decreases. And in the increased number of nodes the performances of CSMA/CA protocol also increases for using the RTS/CTS condition. So the assumption of using RTS/CTS in the CSMA/CA protocol in every condition provides much efficiency is proven here.

6. CONCLUSION

With the simulation graphs and explanations, checking the respected theories we can conclude that using RTS/CTS in CSMA/CA protocol is efficient. Because in the WLAN we would like to get as much higher the transmission to get as possible and lower the collision among the different nodes. We can see the clear evidence that we have given from our simulation of the CSMA/CA protocol that without using RTS/CTS in the protocol gives the much poor result in the transmission and collision. But if we use RTS/CTS the transmission increases as well as the collision decreases. And in the increased number of nodes the performances of CSMA/CA protocol also increases for using the RTS/CTS condition. Thus the assumption of using RTS/CTS in the CSMA/CA protocol in every condition provides much efficiency is proven in this part.

7. FUTURE WORK

For this way when RTS and CTS are used, then huge number of frame or data is saved and collision can be avoided. So, we will try to better solution in future that will decrease data or packet loss and achieve highly motivated the carrier sense multiple access with collision avoidance.

8. REFERENCES

[1] ANSI/IEEE Standard 802.11. Piscataway, NJ: LAN MAN society, IEEE Computer Society.Copyright 1999. Available online http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf

[2] Li, Keyong and Sherzai, Mohammed. Wireless MAC 802.11. Unpublished work, Final paper for SC 546, Fall 2001. Available online at http://courseinfo.bu.edu/courses/02fallengsc546_a1/coursedocuments/a349b830b c631d6136de00600832de87/paper/final paper.doc .

[3] IEEE 802.11 WG, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std. 802.11, 1999

[4] IEEE 802.11 WG,"Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: medium access control (MAC) quality of service (QoS) enhancements," IEEE 802.11e D8.0, Feb. 2004.

[5] Carrier Sense Multiple Access with Collision Avoidance, Available online at http://www2.cs.uidaho.edu/~oman/SC&CI/CSMA-CA-collisions_Bonaventure.pdf

[6] Wireless LAN Networking White Paper. http://support.usr.com/download/whitepapers/wireless-wp.pdf (for CSMA/CA)

[7] Working principle of CSMA/CA. http://ilovewifi.blogspot.com/2012/08/how-80211-csmaca-works.html (working principle of CSMA/CA)

[8] Throughput Modelling and Fairness Issues In CSMA/CA Based Ad-Hoc Networks. By Xin Wang and Koushik Kar.http://www.ecse.rpi.edu/homepages/koushik/mypapers/infocom05-csma.pdf

[9] CSMA/CA https://www.google.com.bd/search?q=+CSMA/CA&ie=utf-8&oe=utf-8&rls=org.mozilla:en-US:official&client=firefox-a&gws_rd=cr&ei=d8OtU9WAJ9WMuATltoKoCw CSMA/CA

[10] C. H. Yeh, "A collision-controlled MAC protocol for mobile adhoc networks and multihop wireless LANs" to be appeared in Proceeding of IEEE Global Telecommunications Conference, 2004.

[11] Source URL: https://scm.info.ucl.ac.be/release/cnp3/Book/0.2/html/lan/lan.html#carrier-sense-multiple-access-with-collision Avoidance.

[12] CS402: COMPUTER COMMUNICATIONS AND NETWORKShttp://www.saylor.org/courses/cs402(Computer Science 402)

[13] Wireless Medium Access Control (MAC) and physical layer (PHY)specifications: Amendment: ESS Mesh networking. IEEE P802.11s/D1.00(Nov. 2006).

[14] Sunday, N. (2008). Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures. *Blekinge Institute of Technology School of Engineering*, (August).

[15] C. H. Yeh, "A collision-controlled MAC protocol for mobile adhoc networks and multihop wireless LANs" to be appeared in Proceeding of IEEE Global Telecommunications Conference, 2004.

[16] S. Ray, J. B. Carruthers, and D. Starobinski, "RTS/CTS-induced congestion in ad hoc wireless LANs", WCNC, 2003.