MEDIUM ACCESS CONTROL (MAC) PROTOCOL IN WIRELESS NETWORK: A REVIEW

Vigneswara Rao Gannapathy[1], Ahamed Fayeez Bin Tuani Ibrahim[2], Zahriladha Bin Zakaria[3], Mohamad Kadim Bin Suaidi[4]

[1]*Lecturer, Department of Electronics and Computer Engineering, Universiti Teknikal Malaysia Melaka, Melaka (UTeM), Malaysia*
[2]*Lecturer, Department of Electronics and Computer Engineering, Universiti Teknikal Malaysia Melaka, Melaka (UTeM), Malaysia*
[3]*Lecturer, Department of Electronics and Computer Engineering, Universiti Teknikal Malaysia Melaka, Melaka (UTeM), Malaysia*
[4]*Professor & Vice Chancellor (VC) of Universiti Malaysia Sarawak (UNIMAS)*

Abstract

The communication medium (i.e. channel) is tuned to the same frequency to enable all the nodes to communicate between each other in wireless network. Therefore, a common channel is shared by all nodes to pass or transmit their information and to establish communication with common neighboring nodes. Due to this reason, only one node (transmission) is allowed to transmit at ones and the rest of the nodes in a network need to be in an idle (i.e. silent) mode. Otherwise, if more than one node commits into transmission at the same time, then it will leads to collision and transmission failure. In order to regulate and prevent such collision and transmission failure, the regulation protocol, known as Medium Access Control (MAC) is used in wireless network. Since 1970, various MAC protocols was used and employed to regulate the communication in the network. This article presents an exhaustive review of MAC protocols, the operation of each protocol, and its advantages and disadvantages. Other than that, a typical MAC protocol used in IEEE 802.11 standard wireless networks such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) also explained and presented in this article.

Keywords: *Medium Access Control (MAC), ALOHA, CSMA, CSMA/CA, Random Access Protocol, Contention Based Protocol*

----------***----------

1. INTRODUCTION

The MAC protocol is one of the major and important components in the wireless communication where the information is distributed over a common channel. As the channel is shared by all the nodes in the network, thus a regulation to access the channel is important. In the wireless network, this regulation will be regulated by MAC protocol. The MAC protocol will enforce a fair sharing and equal right to access the channel. The following section will explain the MAC protocols which are exist in the literature. IEEE 802.11 [1] defined the standard of the MAC and physical layer protocols which are exist in the literature.

A MAC protocol regulates an equal access to the shared channel by providing the rules that allows all nodes in the network to transfer the information in an orderly and efficient manner. In other word this mechanism tries to provide fair bandwidth sharing to all the contending nodes in the network.

Various MAC protocols are developed to regulate the communication in the network. Figure 1 shows the taxonomy of MAC protocols. In contention free protocols such as TDMA, FDMA or CDMA, certain assignments as shown in [2] [3] are used to avoid contention among the nodes.

Contention based protocols, on other hand, was designed to provide efficient contention among the nodes in the network. In a contention based MAC protocol, all nodes contend for access to share the wireless channel. A packet transmission is considered successful when only one node is committing into the transmission at one time. If a simultaneous transmission is occurred on the channel (i.e. more than one node committing into transmission), then it will leads to the collision. In order to avoid this collision, the contention resolution algorithm is invoked. The role of the contention resolution algorithms is very important in effectively utilizing the channel resources.

The survey of contention based MAC protocols were focused in this paper because the contention free MAC protocols are applicable to the centralized control networks.

2. RANDOM ACCESS CONTENTION BASED PROTOCOLS

Random access protocols are commonly implemented protocols in the wireless communication. Almost all protocols used in wireless communication are based on these schemes. One main characteristic of random access protocol is its arbitrariness on accessing the channel. Due to its random access characteristic (i.e. a transmission is committed without the permission of other potential nodes in the network), thus it leads to collision and makes the transmission unsuccessful. When a simultaneous transmission is take place on the channel (i.e. more than one node committing into transmission at the same selected time), a collisions will occurs and no useful information will be received by the receiver. Such as unsuccessful transmission requires retransmission until the packet/information successfully reach at receiver.

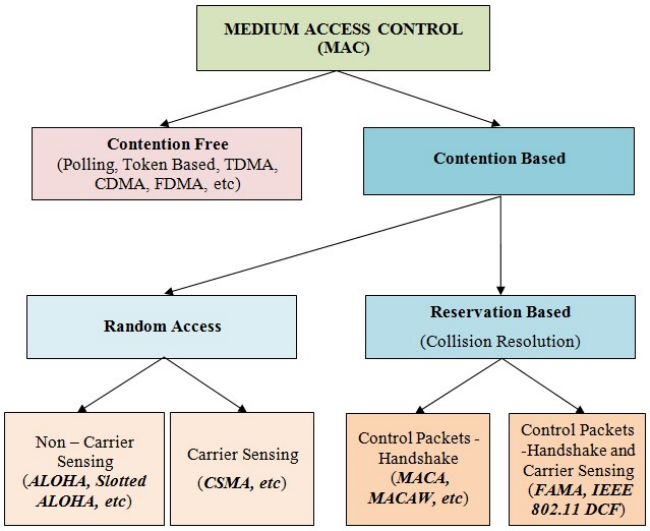

Fig -1: Taxonomy of MAC Protocol

In the random access protocols, the retransmission is scheduled according to randomly selected time slot. The concept of randomness in selecting the time slot is introduced in these protocols to avoid the collision caused by other nodes who attempt to retransmit at the same selected time. This is managed by retransmission algorithm which is responsible for retransmit the collided transmission in different selected time slot so that the collision can be reduced. However, the chance for the retransmitted packet to suffer in further collisions is still high especially when the number of the nodes in the network is increase. Due to this reason, the random access protocols perform poorly and its throughput degrade significantly. Some important random access protocols are described in the following section.

2.1 Pure ALOHA MAC Protocol

Wireless MAC protocol has been studied broadly since 1970s. ALOHA [4] is the first random access protocol proposed for packet transmission in satellite communication network. It was initially designed to provide random access communications between the nodes in a wireless network. It is very simple protocol in which a node commences the transmission immediately whenever it has DATA packet to transmit. This transmission happens immediately without prior notification.

Collisions are very common in ALOHA protocol and some form of feedback mechanism are needed to ensure packet delivery. The feedback mechanism such as an acknowledgement control packet (ACK) will be transmitted back by the receiver upon successfully received a packet without error. When two or more nodes initiate their transmission at same time in common transmission channel, a collision occurs and the packet might be lost. In this case, the collided transmission must be scheduled at a randomly selected times for retransmission according to retransmission algorithm. Due to the random times retransmission is selected independently, the chances of repeated collision can be minimized. Figure 2 is shows a pure ALOHA system. The shaded portion in Figure 2 denotes a collision that occurs when more than one transmission takes place at selected time.

However some researchers [5] disclose that no retransmission algorithm is specified in ALOHA. The node which is implemented with ALOHA protocol does nothing if its transmission suffer a collision. Due to this reasons, the maximum throughput is quite low for ALOHA. With pure ALOHA method, the maximum achievable throughput is about 18%. It means about 82% of total available bandwidth was wasted due to losses from packet collision when using pure ALOHA [6]. This is because the performance of pure ALOHA degrades significantly when the traffic load is heavy. Since all nodes shared the same medium, the transmission which is happens without considering transmission at other nodes, leads to collision and degrades the performance of pure ALOHA significantly.

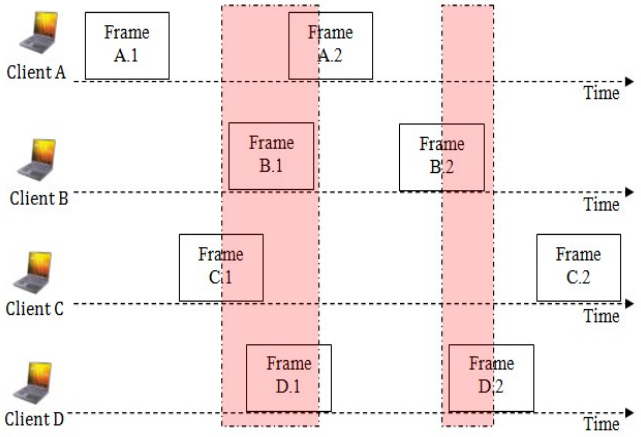

Fig -2: Pure ALOHA MAC Protocol

2.2 Slotted ALOHA MAC Protocol

The slotted ALOHA is the enhanced version of pure ALOHA. This protocol was designed by making a small restriction in the packet transmission freedom which was given to pure ALOHA. This is done by forcing each node to

wait until the beginning of a slot before commencing into packet transmission. The main idea of this improved version is the time is divided into slots and the packet transmission is restricted. In this method, the local clock at each node is used to synchronize the divided time slots. All the nodes in the network will defer their transmission until the beginning of next time slot if they have packet to transmit. The packet transmission will take place within a slot to ensure that it is not collided with another packet that is coming from other node in the same network. Since the packets are only allowed to transmit at specific time (i.e. beginning of time slot), it is cutting the vulnerable period for packet collision in half and doubles the throughput. Figure 3 is shows a slotted ALOHA system.

The bandwidth utilization of the slotted ALOHA system is twice compared to pure ALOHA system. This is because its restriction on packet transmission. The maximum bandwidth utilization that can be achieved by slotted ALOHA is about 37% compare to pure ALOHA system which can only achieve about 18%. [6], shows the performance curves of pure and slotted ALOHA and proved that the maximum throughputs for both systems are equal to 0.184 and 0.368, respectively.

Even though the slotted ALOHA outperformed the pure ALOHA, but the maximum bandwidth utilization that is attained by either pure ALOHA or slotted ALOHA is only small portion of the total available bandwidth. The main cause of this poor bandwidth utilization is because all the nodes in the network tend to initiates its transmission without considering transmission of other nodes. The ALOHA system does not take the state of the channel into account before initiates its transmission. This approach will leads to high collisions.

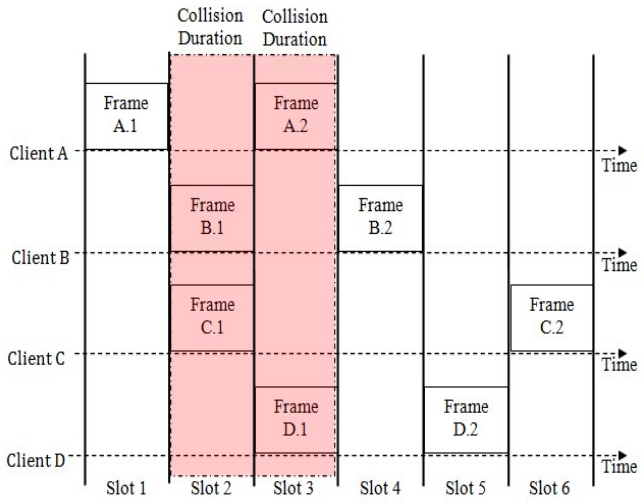

Fig -3: Slotted ALOHA MAC Protocol

For example, any nodes in the network may commit into a new transmission when there is another ongoing packet transmission on the channel. This new transmission will be collided with the ongoing transmission due to shared channel. The better throughput could be achieved if prevent such as potential collision by simply listening to the channel before commit into packet transmission.

This operation sometimes called as "listen before transmit". This is another way that has been envisioned by the researcher in order to improve throughput and support high speed communication networks. In this way, the collisions could be avoided and can boost the throughput, such as scheme known as Carrier Sense Multiple Access (CSMA) protocol.

2.3 Carrier Sense Multiple Access (CSMA)

According to CSMA protocol, each node that implemented with this protocol has a capability to sense the transmission of all other nodes which is within its one hop neighborhood in the network. Sometimes it is referred as physical sensing mechanism where uses a technique called carrier sense to increase the bandwidth utilization and to boost the throughput by cutting the vulnerable period for packet collision.

Carrier sense describe that a transmitter at specific node listen to a carrier before commence into the transmission. This is done by detecting the presence of encode signal which is comes from another nodes in the network. If any other carrier sensed in the channel, then the node will defer its transmission and wait until the presence of encode signal ends (i.e. ongoing transmission to finish). If no carrier is sensed in the channel, then the node will initiate its transmission. Multiple nodes are transmitting and receiving the packet on the shared channel (Multiple Access) and the transmission can be heard by all other nodes in the same network.

The CSMA method is assured that none of the ongoing transmission will be destroyed by collision if all the nodes in the network sense the channel before commence into transmission. However, in the real communication system, the collisions still might be happen when two or more nodes start sense the carrier and begin their transmission at the same time. For example, the idle channel will be detected by all neighboring nodes if the ongoing signal hasn't propagated to them yet. Thus, the neighboring nodes will begin their transmission as well upon the idle channel is detected. The transmission from these nodes will be collided with ongoing transmission. This is due to the signal propagation delay where the nodes might not be aware of other transmission at that instant time [7].

Variants of basic CSMA protocols have been proposed in order to solve this type of collisions. One of the techniques that have been introduced is deferring technique. In the CSMA protocols, various schemes are used to defer the transmission when the nodes sense a busy channel.

There are three basic schemes which are distinguished by their performance when busy channel is detected. These schemes are so called as persistent, non-persistent, and p-persistent which are summarized in Figure 4.

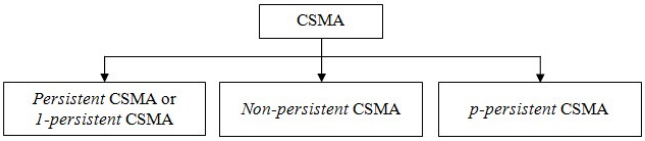

Fig -4: CSMA Based MAC Protocols

2.3.1 Persistent CSMA

In the persistent CSMA scheme, when a node has DATA packet to be transmitted, it will sense the channel first before commit into the transmission. If there is any presence of carrier is detected in the channel, the node which is implemented with persistent CSMA will continuously sense the channel until the transmission on the channel ends. Once the idle state is detected on the channel, then the node immediately transmits a packet.

Since the packet transmission take place immediately after the idle state is detected, so this protocol is called as 1-persistent CSMA (i.e. transmits its packet immediately with probability 1 upon idle channel detection). In this type protocol, the collision might be occurred when several nodes are waits for idle channel detection. Hence, upon idle channel detection, all these nodes will immediately transmit their packet at the same time and leads to higher collision [8]. The non-persistent CSMA is the protocol to reduce the chances of such collisions by introducing a new technique so called randomization.

2.3.2 Non-persistent CSMA

According to this protocol, when a node has DATA packet to transmit, it will starts the carrier sense. When the presence of the carrier is detected in the channel (i.e. channel sensed busy), the node does not continuously monitor the channel to find out the transmission activity, instead it will wait for certain amount of time which is selected randomly and then only starts with carrier sense again. If idle channel is sensed at that point, then it will commit into the transmission immediately. Otherwise, if the channel is still busy, then the waiting process is repeated by exponentially increase the random interval until the channel is found idle.

By using this method, the probability that several nodes immediately begin the transmission, upon idle channel detection can be reduced. The waiting time (i.e. randomization) is the key enhancement that discover in this protocol to provide a system with high throughput.

Since the nodes in non-persistent CSMA protocol does not continuously monitor a channel, thus this protocol results in longer delay compare to 1-persistent CSMA. This delay due to characteristic of non-persistent CSMA in which it will reschedules its transmission some later time in future upon busy channel detection. However, it can achieve a higher bandwidth utilization and throughput because it able to handles the channel accessing problems better than 1-persistent CSMA as described in [6]. The differences of both non-persistent and 1-persistent CSMA are as illustrated in table.

Table -1: Different Between Persistent and Non-persistent Based CSMA

Persistent CSMA	Non-persistent CSMA
If has packet to transmit, sense the channel first.	If has packet to transmit, sense the channel first.
If busy channel is detected, keep on sensing the channel until the channel become idle.	If busy channel is detected, wait for random amount of time and then sense the channel again.
Once idle channel detected, commence the transmission immediately without further delay.	Once idle channel detected, commence the transmission immediately without further delay.
The sender node will wait for random amount of time and begin the transmission again if the collision is occurred.	The sender node will wait for random amount of time and sense the channel again if the collision is occurred.

2.3.3 p-persistent CSMA

The p-persistent CSMA protocol is the cooperation of 1-persistent and non-persistent CSMA. The channel is slotted in the p-persistent CSMA protocol. Each slot size is equal to maximum propagation delay. In this protocol, the nodes only sense the channel at the beginning of each slot when it has a packet to transmit. If the channel is sensed busy, then the node waits until next slot and sense the channel again. If the channel is detected idle at this point, then the node transmits with the probability p or defers the transmission with probably (1- p) until the next slot. If in case the collision occurs, then the node that employed with this protocol will waits for random time and starts all over the process again.

The following example shows the simple analogy how p-persistent CSMA protocol works. Let's assume the node implemented with 0.5-persistent CSMA, the node flips a hypothetical coin to generate random number; i.e. head or tail. If its head, then it transmits packet immediately otherwise if its tail, then it will defer its transmission for predefined time period and sense the channel again.

3. CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD)

The performance of CSMA protocol is further enhanced by enabling the capability of collision detection. Apart from the sensing capability (i.e. before initiates the transmission), the improved version of CSMA is also added with the extra feature to detect a collision during the transmission. This protocol is known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Figure 5 illustrated the flow chart of CSMA/CD method.

This protocol is also referred as "listen while transmit". Each node which is implemented with this protocol is equipped with interference detector. The main function of this interference detector is to perform the collision

detection operation by detecting the signals on the broadcast channel. The system will identify the collision occurrence by comparing the detected signal with the transmitted signal. If there are any different between the detected signal and the transmitted signal, then the protocol will assume a collision is occurred on channel and the node will terminate this transmission immediately. Thus, this mechanism reduces the collision probability of second retry.

A part from that, this quickly aborting feature also reduces the duration of a collision and frees up the channel for other users or nodes without further delay. This is impossible with typical CSMA protocol where the packet will be transmitted completely even though they collided. Such wastage of the channel for entire packet time can be solved by implement collision detection feature. The main idea of this protocol is to terminate the ongoing transmission immediately upon it detects the collision.

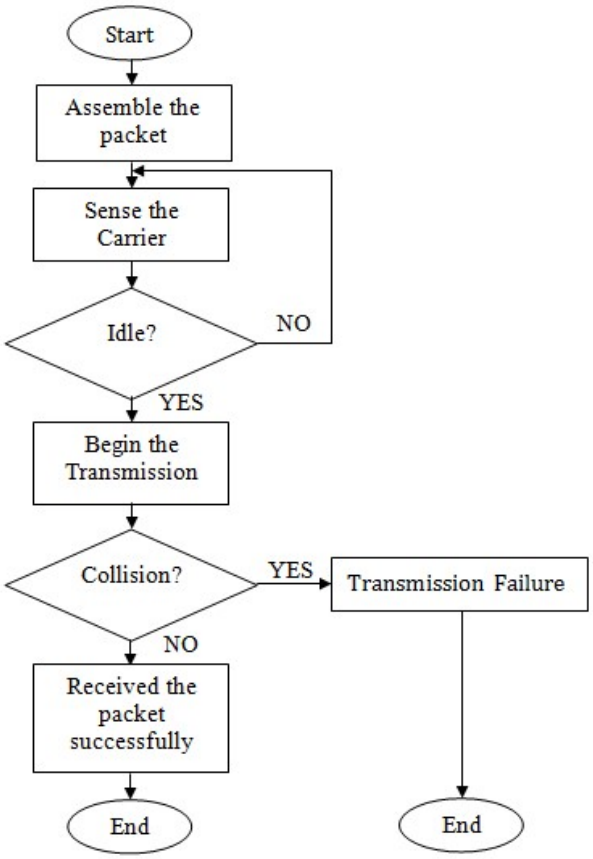

Fig -5: Flow Chart of CSMA/CD Protocol

The main different between CSMA compare to CSMA/CD protocol is the CSMA proposed to minimize the number of collisions while CSMA/CD proposed to detect the collisions as it make the channel ready to be used for other node as soon as possible upon collision is detected. Even though both CSMA and CSMA/CD protocols prevent the collisions by listening to the carrier in the range of the transmitter, yet these protocols perform very poorly to avoid collisions at receiver. The following section will explain on the problems arise in the communication when implemented the CSMA based protocols. Then other the protocols which is proposed to solved all those problems is clearly explained.

4. RESERVATION-BASED CONTENTION PROTOCOLS

In a common channel MAC protocol, the network nodes shared the medium for their packet transmission. In such as protocol, the collisions are considered as instinctive attribute. For example the CSMA protocol is only designed to prevent the collision by listening to the carrier in the range of the transmitter. However, the collisions at the receiver are still remaining unsolved. Two nodes which are out of communication range between each other will transmit simultaneously to the same receiver and will both fail due to collision. These collisions will leads to throughput degradation. For better understanding let's reflect on a network formed by three nodes; node A, B and router R1 as shown in Figure 6.

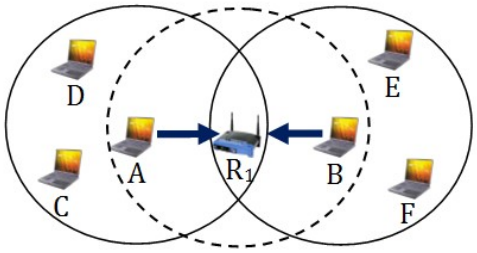

Fig -6: Illustrations of Hidden Node Problems

The circle around each specific node shows its communication range. Assume that node A and node B have DATA packet to be transmitted to router R_1. Based on CSMA protocol both nodes have to sense the channel before attempt its DATA transmission to node R_1. At this point, the nodes will start their DATA transmission if idle channel is detected, otherwise if busy channel is detected then they will defer their transmission. Since both node A and node B are out of communication range between each other, so they begin their transmission to node R_1 at the same time upon idle channel detection. This transmission will leads to collision because node B unaware the ongoing transmission from node A to router R_1 and initiates its transmission to this common neighbor simultaneously. The entire frame which is involved in a collision must be retransmitted. This will degrade the network throughput significantly. The transmission of node A is considered hidden to node B and this referred as hidden node problem [9].

To enable the node R_1 receive both DATA packet successfully without the collision, node B should defer its transmission. This is possible by expanding the communication range of nodes by increasing the transmitting power. However, if the destination of node B is not R_1, so there is no reason to defer the transmission. This solution with leads to interference related problems and significantly degrade the performance. Moreover, the CSMA-based protocol also continuously suffers from the exposed node problem. Let's assume node A has DATA

packet to be transmitted to router R_1 and node B has DATA packet to be transmitted to router R_2 at the same time. The scenario is as shown in Figure 7. Both nodes (i.e. node A and B) will sense the channel accordingly before commence into the transmission. Due to random backoff characteristic, node A managed to grabs the channel and initiates its transmission. Since node B is in the communication range of node A, so it detects the carrier (i.e. channel sensed busy) results from the ongoing transmission from node A to R_1. Upon busy state detection, node B will defer its transmission to router R_2. Node B is considered exposed to the transmission of node A. The proper mechanism is required to regulate the shared channel to solve both hidden and exposed problems.

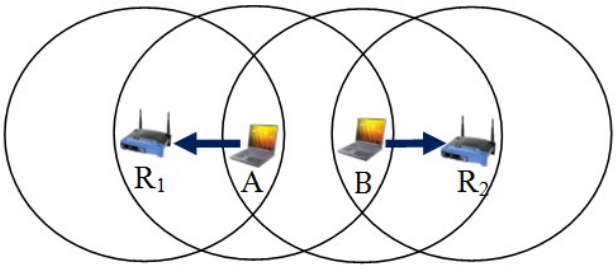

Fig -7: Illustrations of Exposed Node Problems

In order to address all the above MAC issues the research community proposed a number of reservation based collision resolution MAC protocols. This reservation based collision resolution protocols was introduced to eliminate the hidden node problem and to alleviate the exposed node problem. The protocol is required to exchange signaling packets (handshakes) before begin the DATA packet transmission. Sometimes it is referred as virtual carrier sensing where the transmitter and receiver of each node on the network will performs and exchange of control or signaling packets to reserve the channel prior the DATA packet transmission could commence.

Based on this mechanism, many well known protocols have been proposed. The Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol has been selected by IEEE 802.11 standard to be used in wireless LANs [1]. CSMA/CA is random access protocol which was derived from Floor Acquisition Multiple Access (FAMA) which was presented by Fullmer [10]. This is enhanced version of Multiple Access with Collision Avoidance for Wireless LANs (MACAW) which was presented by [11]. MACAW protocol is based on Multiple Access with Collision Avoidance (MACA) protocol which is originally proposed by [12].

4.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) Mechanism

CSMA/CA is the contention based MAC protocol and it is widely implemented protocol in wireless networks. The CSMA/CA is also defined in the IEEE 802.11 standard [1]. This protocol is an enhanced version of FAMA which was proposed to sense the carrier (CS) prior initiates the transmission. A sender node which is implemented with this protocol will sense the channel to check the transmission activities on channel. The node will proceeds with its transmission if the channel is sensed idle for a particular amount of time so called Distributed Inter-Frame Space (DIFS). Otherwise, if the channel is sensed busy, then it will defer its transmission until the channel is free for the transmission.

Upon idle channel detected, instead transmit the packet immediately, the sender node will choose back-off interval randomly. If the channel is idle, then the back-off interval will start decrement otherwise if the channel is busy, then the back-ff interval will freeze. According to back-off procedure, the frozen back-off interval will start decrement again after the channel is sensed idle for longer than DIFS. The sender node transmits the packet immediately when its back-off interval expires or reaches zero.

The hidden node problem is solved by CSMA/CA protocol by using RTS and CTS control packets. After the proper back-off and physical carrier sensing process, instead transmitting the DATA packet immediately, the sender node will reserve the channel by sending out RTS control packet to the destination node. After successfully received the RTS control packet, the destination node will remain silent for a SIFS interval, then responds with CTS control packet to the sender node. After successfully received the CTS control packet, the sender node will remain silent for the time interval corresponding to a SIFS and then it will begin the DATA packet transmission. All neighboring nodes which overhearing RTS/CTS control packets will defer themselves from sending out any packet until the predicted transmission period which as indicated in duration field of control packets is completed. This is called as Virtual Carrier Sensing method or most of time it is referred as Network Allocation Vector (NAV). Figure 8 illustrated the four- way handshake access method.

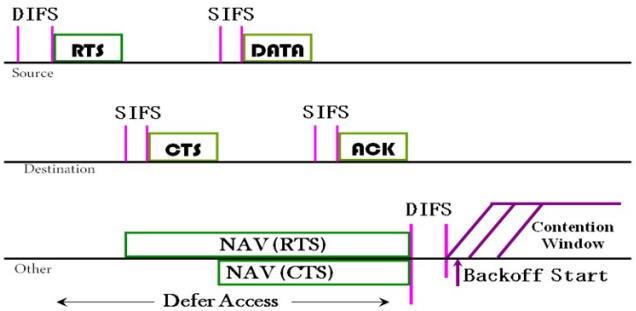

Fig -8: IEEE 802.11 DCF Four way handshake access method

Once the DATA packet successfully received, then the destination node will remain silent for the time interval of SIFS and then initiates an acknowledgment (ACK) control packet. The ACK control packet is used to improve the reliability of DATA packet reception. The priority for the nodes sending an ACK packet is higher than the nodes who want to initiates a new packet transmission because the duration of SIFS is shorter than DIFS. If the ACK is not

received by source node (i.e. ACK_timeout), then the DATA packet is assumed lost and a retransmission according to BEB algorithm will be scheduled.

With the use of RTS-CTS control packets, the collisions caused by the hidden nodes can be eliminated. However, this method requires additional bandwidth which is utilized to transmit RTS and CTS control packets. The throughput achieved by CSMA/CA access method much better compare to basic access mechanism even though it introduced the additional overhead caused by RTS/CTS exchange. This is due to its effectiveness in minimizing the collision which is caused by hidden nodes. In the presence of hidden nodes, the use of RTS/CTS can prevent the collision thus improve the performance of the network.

5. CONCLUSION

In wireless network, Medium Access Control (MAC) protocol plays an important role to regulate an access to all nodes. As a single channel shared by all nodes in wireless network, thus a proper regulation is needed to get an access to the channel efficiently. Besides, the MAC protocol also proposed to enforce a fair sharing among all nodes in the network and provides an equal right to access to the channel. Even though several MAC protocols have been proposed to date, but preventing the collision completely are still not fully satisfied yet. Therefore, still a lot of work has to done in working out a proper MAC protocol which will solve the transmission failure completely.

ACKNOWLEDGEMENT

The authors would like to take this opportunity to thanks those who are contributes directly or indirectly in completion of this article and also for their constructive comments. In addition, the authors also would like to express our gratitude to Universiti Teknikal Malaysia Melaka (UTeM) for the support and encouragement.

REFERENCES

[1] IEEE, Institute of Electrical and Electronics Engineering. IEEE Standard for information Technology – Telecommunications and Information Exchange between Systems – Specific Requirements – Part 5: Token Ring Access Method and Physical Layer Specifications. IEEE, New York. 1998.

[2] Toh, C.K. Ad Hoc Mobile Wireless Networks: Protocol and System. 1st ed., NJ: Prentice Hall PTR. 2002.

[3] Toh, C.K., Vassiliou, V., Guichal, G., & Shih, C.H. MARCH: A Medium Access Control Protocol for Multihop Wireless Ad Hoc Networks. Proceedings of IEEE Military Communication, pp. 512 – 516. 2000.

[4] Abramson, N. The ALOHA system: another alternative for computer communication. In AFIPS Conference Proceedings of Fall Joint Computer Conference. pp. 281-285. 1970.

[5] Foh, C.H. Performance Analysis and Enhancement of MAC Protocols. The University of Melbourne, PHD thesis. 2000.

[6] Agrawal, D.P. Introduction to Wireless and Mobile System. 1st ed., USA: Brook/Cole– Thomson Learning. 2003.

[7] Kaynia, M. & Jindal, N. Performance of ALOHA and CSMA in Spatially Distributed Wireless Networks. IEEE International Conference on Communication (ICC'08), pp. 1108 – 1112. 2008.

[8] Salati, C. An Analysis of Collision in 1-persistent CSMA and a Simple Yet Effective Method to Reduce Them. IEEE Conference on Telecommunication, pp. 240 – 244. 1991.

[9] Tobagi, F., Kleinrock, L. Packet Switching in Radio Channel: Part II – The Hidden Terminal Problem in Carrier Sense Multiple Access and the Busy – Tone Solution. IEEE Transactions on Communication, pp. 1417 – 1433. 1975.

[10] Fullmer, C.L. & Garcia-Luna-Aceves, J.J. Floor Acquisition Multiple Access (FAMA) for packet radio networks. In Conference on Application, Technologies, Architectures and Protocols for Computer Communication (SIGCOMM), pp. 262-273. 1995.

[11] Bharghavan,V., Demers, A., Shenker,S. & Zhang, L. MACAW:A Media Access Protocol for Wireless LANs. Proc.ACM SIGCOMM'94, pp.212-225. 1994.

[12] Karn, P. MACA- A New Channel Access Method for Packet Radio.ARRL/CRRL Amateur Radio 9th Computer Networking Conference,pp.134-140. 1990.

[13] Vigneswara Rao, Gannapathy., Suaidi, Mohamad Kadim., Johal, Muhammad Syahrir Bin., Chuan, Lim Kim., Ramli, Nordin., Mohamad, Hafizal. "A Smooth Forwarding Operation in Wireless Mesh Network," in IEEE 10th Malaysia International Conference on Communications (MICC), pp. 83-87. 2011.

[14] Vigneswara Rao Gannapathy, Tuani Ibrahim, Ahamed Fayeez, Zahriladha Zakaria, Abdul Rani Othman, Nur Qalbi Jalaudin, "A review on various types of Software Defined Radios (SDRs) in radio communication", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163, pISSN: 2321-7308, Volume: 03 Issue: 12, Dec-2014

[15] Vigneswara Rao Gannapathy, Ahamed Fayeez Bin Tuani Ibrahim, Zahriladha Bin Zakaria, Abdul Rani Bin Othman, Mohamad Kadim Bin Suaidi, "Alleviate Exposed Node Issues In Wireless Mesh Network (WMN) Using A Novel Approach Of Concurrent Medium Access Control (C-MAC) Protocol", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163, pISSN: 2321-7308, Volume: 03 Issue: 11, Dec-2014

[16] Vigneswara Rao Gannapathy, Ahamed Fayeez Bin Tuani Ibrahim, Zahriladha Bin Zakaria, Abdul Rani Bin Othman, Anas Abdul Latiff, "Zigbee-Based Smart Fall Detection And Notification System With Wearable Sensor (e-SAFE)" ", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163, pISSN: 2321-7308, Volume: 02 Issue: 08, Dec-2013

[17] Vigneswara Rao Gannapathy, Ahamed Fayeez Bin Tuani Ibrahim, Zahriladha Bin Zakaria, Abdul Rani

Bin Othman, Anas Abdul Latiff, "An Enhancement Of RTS/CTS Control Handshake In CSMA/CA Based MAC Protocol For An Efficient Packet Delivery Over Multi-hop Wireless Mesh Network (WMN)", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163, pISSN: 2321-7308, Volume: 02 Issue: 10, Dec-2013.

[18] A.T.I Fayeez, V.R Gannapathy, S. S. S Ranjit, S.K. Subramaniam, Ida S.Md Isa, "Throughput Analysis Of Energy Aware Routing Protocol For Real-Time Load Distribution In Wireless Sensor Network (WSN)", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163, pISSN: 2321-7308, Volume: 02 Issue: 11, Nov-2013.

BIOGRAPHIES

Vigneswara Rao Gannapathy currently serving as a senior lecturer in Universiti Teknikal Malaysia Melaka (UTeM) and he actively involves in research activities which is related to electronics and wireless networking. His research direction has focused on Wireless Mesh Networks which emerged as a key technology for next-generation wireless networking.

Ahamed Fayeez B Tuani Ibrahim, a Masters holder in Electronics & Telecommunication, is a vivid computer networking enthusiast. His specific research interest includes low power network design and programming. He is a certified Cisco Network Analyst.

Dr. Zahriladha Zakaria, PhD, MIEEE, BEM, Grad IEM is currently working as a senior lecturer at the Faculty of Electronic and Computer Engineering, University Teknikal Malaysia Melaka. (UTeM). His research interests include a variety of microwave device development such as planar and non-planar microwave filters, amplifiers and antennas.

Professor Dato' Dr. Mohamad Kadim Bin Suaidi, PhD, is currently Vice Chancellor (VC) of Universiti Malaysia Sarawak (UNIMAS). His research interests include Optoelectronics, Telecommunication, and Wireless Communication. He has a wide knowledge on high speed optical diagnostics of laser interactions and also on Microstrip Antennas and Arrays