



Asian Journal of Scientific Research

ISSN 1992-1454

science
alert
<http://www.scialert.net>

ANSI*net*
an open access publisher
<http://ansinet.com>

A Novel RTS-CTS Collision Avoidance Algorithm to Improve the QoS in Mobile *Ad hoc* Networks

R. Kalaiarasi and D.Sridharan

Department of Electronics and Communication Engineering, CEG Campus, Anna University, Chennai-600-025, India

Corresponding Author: R. Kalaiarasi, Department of Electronics and Communication Engineering, CEG Campus, Anna University, Chennai-600-025, India Tel: +91-9445811565

ABSTRACT

This study proposes Request-To-Send-Clear To-Send Collision Avoidance algorithm to reduce the RTS-CTS collisions. An RTS collision leads to CTS collisions. During the collisions, misbehaving node does not double the contention window to get more access than well behaved nodes. So performance of the network is degraded. In order to rectify this drawback, RCCA algorithm is proposed. Collision Avoidance Packet is also introduced, which contains the Active Neighbour Bit to know the status of ongoing communications within the transmission range. RCCA algorithm utilizes the Active Neighbour Bit information to avoid the collision in two hop neighbours. Simulation results shows that RCCA algorithm minimizes the number of RTS-CTS collisions, misbehaving nodes, delay and increases the packet delivery ratio and throughput.

Key words: MANET, IEEE 802.11 MAC, RTS-CTS collisions, RCCA algorithm, throughput

INTRODUCTION

Quality of service is one of the most actively studied open issues in communication networks (Phang *et al.*, 2012). Mobile Ad hoc Networks (MANETs) have gained considerable attentions recently due to its mobility and robustness. MANET is an infrastructure less network which communicate via intermediate nodes without any base station (Sugimoto *et al.*, 2010). MANET uses IEEE 802.11 MAC protocol to access the channel within their transmission range. It uses Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) to communicate with the wireless medium. CSMA/CA uses four way handshaking RTS-CTS-DATA-ACK to avoid the collision. It is known that the collisions can be avoided only within the transmission range of each other. Though the CSMA/CA scheme is applied, still the well known hidden terminal problem occurs in MANET (Yang *et al.*, 2009).

Due to limited wireless transmission range, mobility, open network architecture and battery power, secured communication becomes a hard task to be achieved. On using CSMA/CA to the wireless channel, each node should wait for a random period called backoff time. In this situation, malicious node does not follow the IEEE 802.11 MAC protocol rules. Instead, they disobey by choosing either a small backoff value or scrambling CTS and ACK control packets of other nodes in order to increase their CW or choosing smaller Distributed Inter Frame Space (DIFS) (Djahel *et al.*, 2009), or does not double the backoff value after collision (Nagel *et al.*, 2008). Malicious nodes use this opportunity to get more throughput share than well behaved nodes. This degrades the overall network performance.

Yu *et al.* (2006) proposed a CTMAC (Concurrent Transmission) to support concurrent transmission. It includes collision Avoidance information in the control packets to avoid the collisions between DATA and ACK packet. But in CTMAC, each node should maintain Active Neighbor List (ANL) to record the number of active nodes that are scheduling, transmitting and receiving.

Yang *et al.* (2009) suggested a new Dual Channel MAC protocol (DCMAC) that for minimizes collision, provides better channel reservation and simultaneous transmission. Here DTS (Delay to Send) frame is introduced to avoid collision and also reserve the channel. This method needs a separate data and control channel for concurrent transmission and also each node is equipped with two Network Interface Card (NIC). So, additional cost is required to setup the network and also there is no ACK received by the receiver from the sender to acknowledge the data recipient.

Shih *et al.* (2009) proposed a RCA (RTS Collision Avoidance) MAC protocol to evade the RTS collisions caused by the hidden terminal and also warn the hidden stations using narrowband tone channel in order to prevent the RTS collisions in two hop neighbors. So hidden stations freezes the backoff counter until the RTS transmission gets over. In this method, RTS collisions can be avoided but it needs extra pulse/tone channel to prevent the RTS collision. Authors also suggest that RTS collision leads to CTS collision and ACK collisions. Performance of the MAC protocol is greatly affected by the collisions (Moh and Yu, 2011).

RTS-CTS COLLISION AVOIDANCE ALGORITHM (RCCA)

IEEE 802.11 standard specifies two types of access methods namely Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is a basic access method. It is a contention based protocol which uses Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) to communicate with the wireless medium within their transmission range through radio links. DCF uses four way handshaking method to reduce the frame collisions.

Another optional access method is the Point Coordination Function which can communicate to the network through an Access Point (AP) such as base station. It is a contention free communication, but it can be used only in the presence of an AP which gives guaranteed delivery.

In contention based mechanism, each station waits for DIFS interval before attempting to transmit as shown in Fig. 1. If the medium is idle for DIFS interval then it enters into the contention window, which is uniformly chosen between 0 to CW min. CW min is the minimum

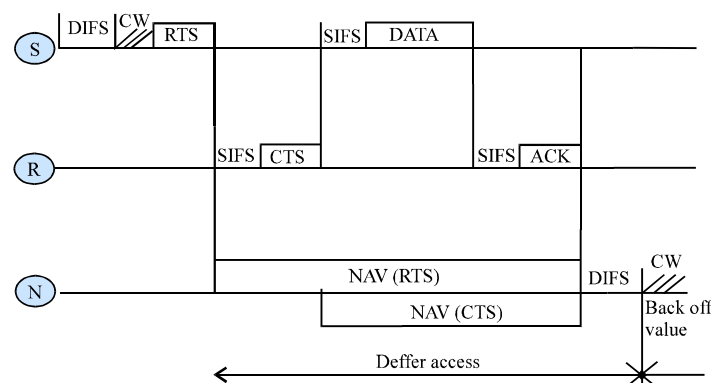


Fig. 1: Institute of electrical and electronics engineers 802.11 RTS/CTS mechanism

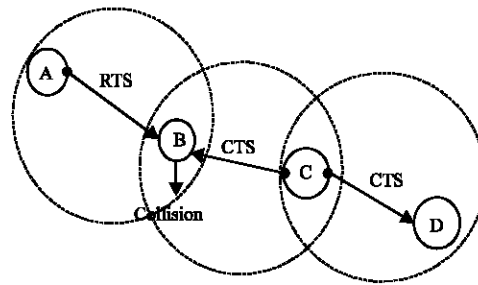


Fig. 2: Example of Request-To-Send-Clear-To-Send collision pattern

contention window. If the station is busy, it should wait for DIFS interval again. During this period, NAV value is greater than zero. If NAV value reaches zero, the station starts to transmit in the medium.

Any station starts the communication by sending the RTS packet to the receiver. Receiver replies with a CTS packet after SIFS interval. After waiting for SIFS interval, transmitter sends DATA to the receiver. Receiver replies with ACK after waiting for a SIFS interval. If ACK is not reached within the maximum time period, sender infers that a collision has occurred. So, sender doubles the CW after each unsuccessful transmission upto CW_{max} and reset to CW_{min} after each successful transmission. CW_{max} is the maximum backoff value.

The performance of the network may be degraded due to selfish or malicious reasons. Selfish nodes may choose small backoff value, when the collision has occurred. When a node is within the transmission range of two nodes, there is a chance for collision. For example, in the Fig. 2. Four nodes want to communicate with each other. D wants to communicate with C and sends a RTS control packets to C. C replies with CTS to D. B and C are within the transmission range of each other. At the same time A, communicates with B and send RTS to B. In this situation, A's RTS packet collides with C's CTS packets. If two or more stations simultaneously transmit RTS frames and CTS frames, they will infer a collision (Konorski, 2007). In this situation, selfish nodes do not double the contention window or choose a small backoff value or assigns large value to NAV to gain more access than well behaved nodes (Djahel and Nait-Abdesselam, 2010).

RCCA MODEL

Consider the network topology with four nodes which are in the transmission range of each other. Here the possibility of RTS/CTS collision cannot be avoided. The proposed algorithm, tries to reduce the possibility of selfish misbehavior taking place in the CW.

In multihop networks, nodes usually uses BEB algorithm on collision and uses backoff counter value to indicate the number of backoff slots. When backoff counter value (BC) reaches zero, nodes start transmitting the packets. In RCCA algorithm, each station sends a special packet called Collision Avoidance Packet (CAP) which contains the information about source address, destination address and Active Neighbour Bit (ANB). Packet format of the CAP packet is shown (Fig. 3). This packet should be sent before two slots in advance.

The RCCA algorithm developed to detect the collisions in two hop neighbours is shown in Fig. 4. It is seen that usually at $BC = 0$, nodes start the communication, but in this protocol, only when the BC value becomes 2, it starts to send the CAP packet to the receiver. CAP packet gives the information about whether any communication is going on within the transmission range. If

Source address (6)	Desination address (6)	Active neighbour bit (ANB) (1)
-----------------------	---------------------------	-----------------------------------

Fig. 3: Frame format of collision avoidance packet

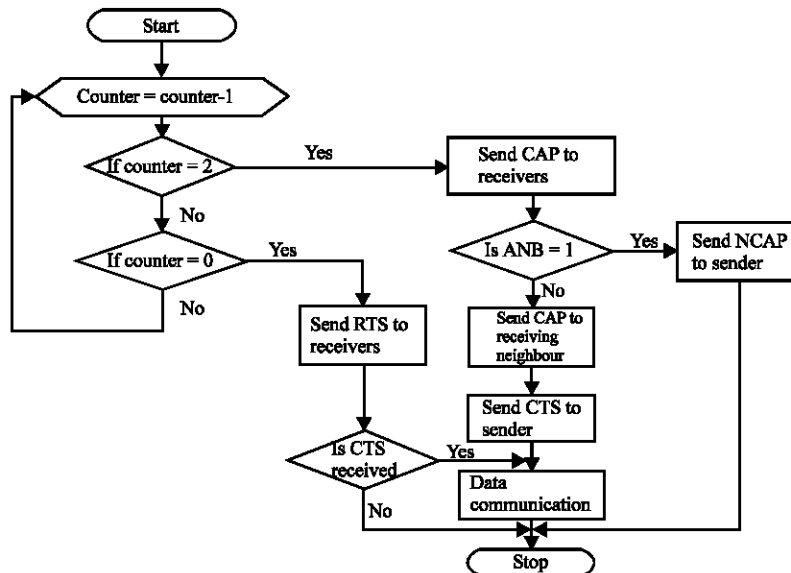


Fig. 4: Flowchart represents the Request-To-Send-Clear-To-Send Collision Avoidance (RCCA) algorithm

yes, then the ANB bit is equal to 1. It sends a Negative Collision Avoidance Packet (NCAP) to the Sender to stop the communication. So, the sender will not send any packet to the receiver till the receiver intimates with a CTS packet. If there is no communication going on within the transmission range of receiver, ANB is set to zero. Now the receiver sends the CAP packet to its neighbouring nodes. After hearing the CAP packet, the neighboring nodes will not disturb the receiver till the data transmission ends. Before the backoff counter reaches zero, the above communication should get over. When the backoff counter reaches zero, it proceeds with the usual RTS-CTS handshake process. From the above proposed method collision can be avoided at the receiver side. The selection of small CW value by selfish nodes can be avoided.

SIMULATION ENVIRONMENT

Network Simulator-2 (NS-2) is used to simulate the above algorithm. Hundred nodes are deployed in a field of area $2000 \times 2000 \text{ m}^2$ randomly. Simulation has been run for 200 sec. The propagation channel of two ray ground reflection model is used as the propagation channel with data rate of 2 Mbps. Source transmits constant Bit Rate (CBR) with UDP traffic at $2 \text{ packets sec}^{-1}$. The data payload of each packet is 210 bytes long. Source destination pairs are randomly selected. Mobile nodes are moved randomly according to the random waypoint mobility model with the node speed of 2 m sec^{-1} . AODV routing protocol is used to find the path for a given source-destination pair (Perkins and Royer, 1999).

RESULTS AND DISCUSSION

Figure 5 shows the throughput of the network as the number of nodes is increased. The RCCA algorithm is compared with the IEEE 802.11 MAC protocol. When the number of nodes increases linearly from 60 to 100, throughput also linearly increasing. The proposed algorithm gives better throughput than the existing MAC protocol. In IEEE 802.11 MAC protocol, when the number of nodes exceeds above 80, throughput is slightly degraded. This is due to the large network size which results in a higher collision probability and significant performance degradation (Raptis *et al.*, 2009). In addition, the performance degradation is eliminated after 90 nodes, thereby proving it to be a better method.

Figure 6 shows the effect of number of nodes with the packet delivery ratio. Packet delivery ratio is linearly increasing in both IEEE 802.11 MAC and proposed protocol. The packet delivery ratio of the RCCA is better than that of the IEEE 802.11 MAC protocol. When the number of nodes goes beyond above 90, PDR is decreased in IEEE 802.11 due to the RTS/CTS exchange signaling (Athanasopoulos *et al.*, 2006). But the RCCA algorithm provides better performance in packet delivery ratio when the number of nodes exceeds above 90.

Figure 7 presents the delay performance of the RCCA algorithm and the IEEE 802.11 MAC. In the graph, the packet delay is considerably lower than the existing protocol. This shows that the proposed algorithm gives better performance. It is observed that the delay is linearly increasing in both the cases when the number of node increases. This is due to the increased network size which leads to a high collision probability (Ling *et al.*, 2010).

Figure 8 illustrates the number of RTS-CTS collisions of IEEE 802.11 MAC and RCCA algorithm when the number of nodes in the network is varied. Both the curve is increased linearly when the number of nodes increases. But proposed algorithm gives lesser RTS-CTS collisions compared to IEEE 802.11 MAC.

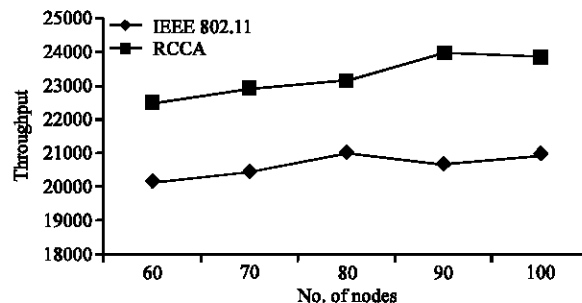


Fig. 5: Number of nodes vs. throughput comparisons of IEEE 802.11 and RCCA

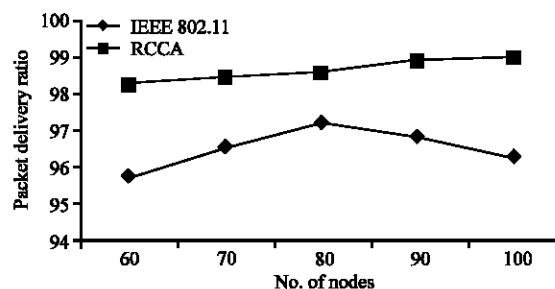


Fig. 6: Number of Nodes vs. packet delivery ratio comparisons of IEEE 802.11 and RCCA

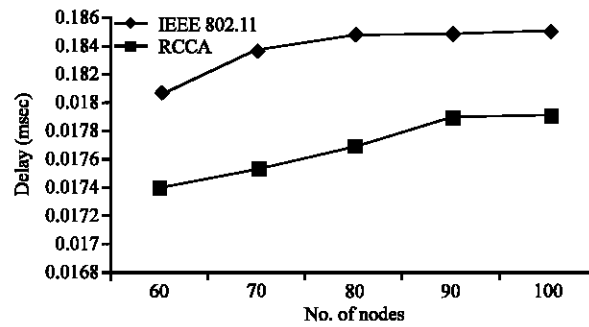


Fig. 7: Number of Nodes vs. delay comparisons of IEEE 802.11 and RCCA

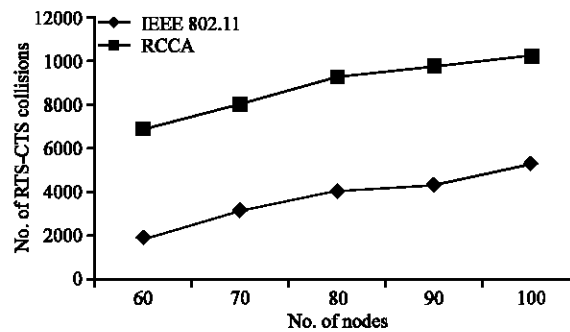


Fig. 8: Number of nodes vs. number of Request-To-Send-Clear-To-Send collisions comparisons of IEEE 802.11 and RCCA

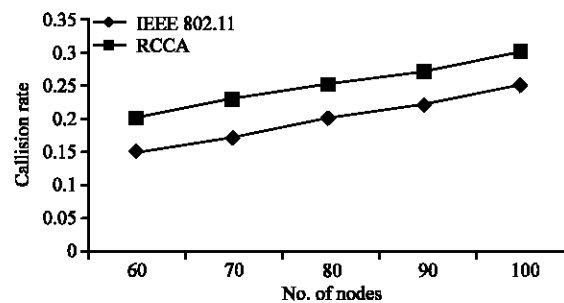


Fig. 9: With and without using RCCA algorithm

Figure 9 shows the collision rate versus number of nodes in the network using with and without the RCCA algorithm. While using proposed algorithm collision rate is considerably reduced. When the network size increases there is a chance for more number of collisions. So, collision rate is linearly increasing with the increasing number of nodes.

CONCLUSION

This study explains about the collisions and their impact on the degradation of MANET performance. An algorithm RTS-CTS Collision Avoidance (RCCA) algorithm is proposed to

reduce the number of RTS-CTS collisions occurring due to RTS collisions in two hop neighbors. Here, CAP packet is introduced, which contains ANB bit. It gives information about two hop neighbor communication status. It is observed that the throughput, packet delivery ratio has increased and delay, number of RTS-CTS collisions is reduced considerably on using RCCA to compared to IEEE 802.11 MAC protocol. Simulation results shows that RCCA algorithm can successfully avoid the RTS-CTS collisions especially in a dense network.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude and appreciation to Department of Science and Technology (DST), New Delhi for funding the project under Women Scientist Scheme (WOS-A).

REFERENCES

- Athanasopoulos, A., E. Topalis, C. Antonopoulos and S. Koubias, 2006. Evaluation analysis of the performance of IEEE 802.11b and IEEE 802.11g standards. Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 23-29, 2006, Morne, Mauritius, pp: 141.
- Djahel, S., F. Nait-Abdesselam and F. Ahsan, 2009. Highlighting the effects of joint MAC layer misbehavior and virtual link attack in wireless ad hoc networks. Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, May 10-13, 2009, Rabat, Morocco, pp: 756-763.
- Djahel, S. and F. Nait-Abdesselam, 2010. Thwarting back-off rules violation in tactical wireless ad hoc networks. Proceedings of the IEEE Symposium on Computers and Communications, June 22-25, 2010, Riccione, Italy, pp: 417-422.
- Konorski, J., 2007. A station strategy to deter backoff attacks in IEEE 802.11 LANs. J. Discrete Algorithms, 5: 436-454.
- Ling, T.C., A. Riza, K.K. Phang and K.P. Hoh, 2010. Improving QOS In WLAN using dynamic weighted fair scheduling. Malaysian J. Comput. Sci., 23: 85-101.
- Moh, S. and C. Yu, 2011. A cooperative diversity-based robust MAC protocol in wireless ad hoc networks. IEEE Trans. Parallel Distrib. Syst., 22: 353-363.
- Nagel, N.R., R. Shokranian, J.L. Bordim and K. Nakano, 2008. MAC layer misbehavior on ad hoc networks. Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, December 17-20, 2008, Shanghai, pp: 538-542.
- Perkins, C. and E. Royer, 1999. Ad hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 25-26, 1999, New Orleans, pp: 90-100.
- Phang, K.K., T.C. Ling and T.F. Ang, 2012. Traffic engineering with rerouting in Diffserv MPLS networks. Malaysian J. Comput. Sci., 25: 122-135.
- Raptis, P., V. Vitsas and K. Paparrizos, 2009. Packet delay metrics for IEEE 802.11 distributed coordination function. Mobile Networks Appl., 14: 772-781.

- Shih, K.P., W.H. Liao, H.C. Chen and C.M. Chou, 2009. On avoiding RTS collisions for IEEE 802.11-based wireless ad hoc networks. *Comput. Commun.*, 32: 69-77.
- Sugimoto, T., N. Komuro, H. Sekiya, S. Sakata and K. Yagyu, 2010. Maximum throughput analysis for RTS/CTS-used IEEE 802.11 DCF in wireless multi-hop networks. *Proceedings of the International Conference on Computer and Communication Engineering*, May 11-12, 2010, Kuala Lumpur, pp: 1-6.
- Yang, X., Y. Huang, W. Yang and S. Yang, 2009. A dual channel MAC protocol for providing high spatial reuse and channel efficiency. *Proceedings of the 1st International Conference on Information Science and Engineering*, December 26-28, 2009, Nanjing, pp: 3930-3935.
- Yu, W., J. Cao, X. Zhou and X. Wang, 2006. A high-throughput MAC protocol for wireless ad hoc networks. *Proceedings of the 4th IEEE International Conference on Pervasive Computing and Communications Workshops*, March 13-17, 2006, Pisa, pp: 405-409.