

A Survey on Modified RTS/CTS Mechanism

Prachi Srivastava
Computer Science and Engineering,
MMMEC, Gorakhpur
prachi.srivastava.itm@gmail.com

Dayashankar Singh
Computer Science and Engineering,
MMMEC, Gorakhpur
dss_mec@yahoo.co.in

Abstract: The Request-to-Send and Clear-to-Send (RTS/CTS) mechanism is widely used in wireless networks in order to transmit data from source to destination in order to reduce packet collisions (due to Hidden node) and, thus, achieve high throughput. It solves problem over carrier sense multiple access (CSMA), but also arises some additional problems that degrade the performance of RTS/CTS mechanism. These problems are “Exposed Node Problem”, “RTS -induced and CTS -induced Problem” and “Masked Node Problem”. In this survey paper, we are going to discuss the problems of RTS/CTS mechanism, and give a modification in RTS/CTS mechanism which overcomes the problem of this mechanism and also increases the performance of RTS/CTS mechanism.

Keywords: Infrastructure wireless network, Ad-hoc network, NAV, CSMA/CA and RTS/CTS.

I. INTRODUCTION

In spite of having line communication the wireless network take place all over the communication system. So Mobile Ad hoc Networks (MANETs) is in higher interest of researchers. A self configured network with wireless connectivity is known as MANETs. A Stranded protocol IEEE 802.11 is has been use in Wireless Local Area Networks (WLANs). IEEE 802.11 specifies Medium Access Control (MAC) for WLANs [1].

The performance of a wireless network depends upon the medium access control (MAC) protocol used. Carrier Sense Multiple Access (CSMA) protocol is often chosen because of its simplicity and scalability. However, CSMA is inclined to the hidden node problem [3], especially in ad hoc networks where a node may communicate directly with other node in range [4, 5]. Hidden nodes cause packet collisions and thus considerably affect network performance. In order to conflict the hidden node problem, a mechanism known as RTS/CTS handshake is often used. The RTS/CTS mechanism was initially proposed in [7] in a protocol called Multiple Access with Collision Avoidance (MACA). In [2], the authors proposed a modified version of MACA, MACA for Wireless (MACAW), which includes a MAC level acknowledgment (ACK). IEEE 802.11 standard uses a variant of MACAW along with CSMA.

From a network point of view, one of the primary reasons for using the RTS/CTS mechanism is to avoid network congestion resulting from frequent packet collisions. The *RTS/CTS* mechanism generally works well in infrastructure-based networks, even though it may lead to unfairness in some situations [6]. However, in the general setting of ad hoc networks, the current way of implementing the *RTS/CTS* mechanism gives rise to situations where a large number of nodes are unable to transmit any packet. These situations can lead to network-level congestion. Therefore, the *RTS/CTS* mechanism fails to achieve its goal from a network point of view.

The remaining paper is organized as follows. In section II *RTS/CTS* mechanism is discussed with associated problem. In section III literature survey is discussed in which various modifications in *RTS/CTS* mechanism along with advantages and disadvantages. Section IV introduced proposed work that modifies *RTS/CTS* mechanism to solve the problem associated with *RTS/CTS* mechanism. Finally section V concludes the survey paper.

II. RTS/CTS MECHANISM

To reduce the collisions due to hidden nodes in CSMA/CA protocol, *RTS/CTS* handshake was introduced. According to this mechanism before actual data transfer, sender and receiver exchange *RTS/CTS* packets to reserve the channel for data transmission. It is also called virtual carrier sensing because in this mechanism nodes get the information about the state of channel by exchanging a pair of control packets, rather than sensing the channel physically. When node A has data to send to node B, it first sends *RTS* packet to node B in which node A fills the address of node B and time required to complete data transmission. On receiving *RTS* packet from node A, node B replies with *CTS* packets. The *RTS* of A is also received by node C because node C is also in transmission range of A. Node C determines that it is not the intended receiver so it blocks itself from accessing the channel by setting a timer known as Network Allocation Vector (NAV). During this blocking state node C can neither start any data transmission nor reply to any *RTS* packet of any other node in its neighbourhood. D is a node that is in transmission range of node B and receives the *CTS* packet of B. So D will also set a NAV timer to

prevent any data transmission during the transmission of data from node A to node B. NAV is a counter that decreases constantly and initialized to a value stored in RTS or CTS packet. The timer set by node C is called RTS NAV timer and the timer set by node D is called CTS NAV timer. Now node A starts actual data transmission to B. After receiving the complete data accurately, node B replies with acknowledgement ACK packet to indicate the success of transmission. Now node C and D will unblock themselves.

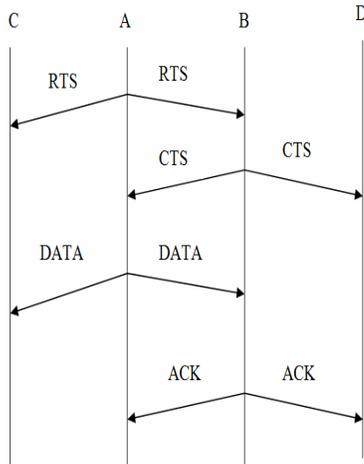


Fig 2: RTS/CTS mechanism

The RTS/CTS mechanism gives some additional problems that are discussed below:

2.1. Exposed Node Problem

An exposed node is one that is within the range of sender but out of the range of receiver. These nodes cause underutilization of bandwidth. Assume that there are four nodes A, B, C, and D as shown in Figure 2.1. The dotted circle denotes their communication ranges. Let us assume that node C is communicating to node D. And suppose node B wants to transmit to node A. Node B senses the channel to be busy and could not transmit to A. Although this transmission would not cause a collision at D, but B is prevented from transmitting. The node B is an exposed node. It results inefficient bandwidth utilization at node B. This problem is called exposed problem. Hidden and exposed problems can occur frequently in ad hoc network causing a significant degradation in the network throughput.

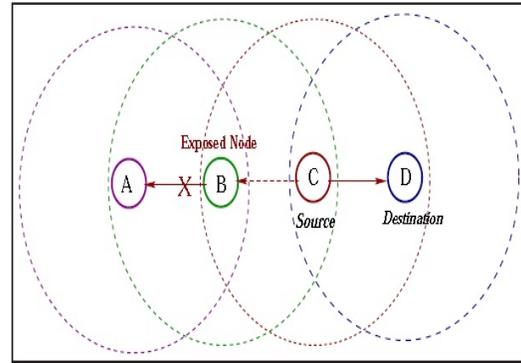


Fig 2.1 Exposed Node Problem

2.2 Masked Node Problem:

This is the case in which RTS/CTS mechanism fails to solve the hidden node problem. The reason for this situation is based on the fact that CTS sent by a node may not always be heard by its neighbour because the later might be already blocked due to any previously started transmission in its neighbourhood. This is illustrated in following figures:

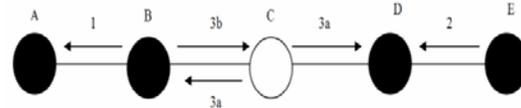


Fig 2.2: Masked Node Problem

First, node B starts sending data to node A. During this transmission node C is blocked. If node E sends data to node D at the same time then node C will not be able to hear CTS of node D. Node C is masked to data transmission of node D. Meanwhile, if data transmission of node B ends then node C is free to do any transmission. This may cause collision at node D. If node C starts its communication with node B then after some time node D may interrupt this transmission. Now node D will be masked node.

In this way the exchange of the role of “masked node” may continue between C and D. They will go on destroying data packets of each other again and again without knowing its reason. So we can say that masked node problem also decreases the number of successful transmissions.

2.3 RTS-induced and CTS-induced Problem

To overcome the hidden and exposed problem, IEEE 802.11 DCF, uses a mechanism called Network Allocation Vector (NAV) [1, 2, 8]. Nodes overhearing either RTS or CTS set their NAV respectively, and defer their channel access for the

expected time to finish the packet transmission. Problems arise when the RTS or CTS packet is not correctly received at receiver or sender node respectively, which causes underutilization of channel bandwidth due to NAV setting. These are termed as RTS-induced and CTS-induced problem [9].

The RTS-induced problem occurs when the RTS packet is not correctly received at the receiver node. Assume that there are four nodes A, B, C, and D as shown in Figure 2.3.1. Node C initiates its transmission by sending an RTS packet to node D. Upon hearing RTS from node C, node B sets its NAV to the expected time required to finish the transmission. If the reception of RTS fails at D, the transmission from node B is unnecessarily deferred for a period as set in its NAV. The RTS-induced problem is depicted in Figure 2.3.1. Similarly, CTS-induced problem occurs when the CTS packet is not correctly received at the sender node. Assume that there are four nodes A, B, C, and D as shown in Figure 2.3.2. Node A initiates its transmission by sending an RTS packet to node B. The node B sends CTS to node A, as a response to the RTS packet. Upon hearing the CTS packet from node B, node C sets its NAV to the expected time required to finish the transmission. If the reception of CTS fails at node A, transmission from node C is unnecessarily deferred for a period equal to the setting in NAV.

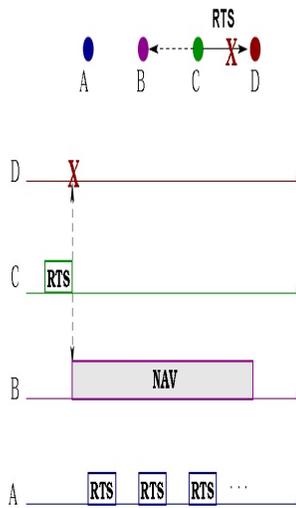


Fig 2.3.1 RTS-induced Problem

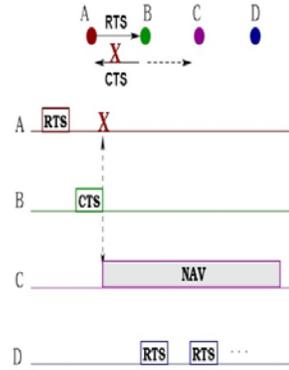


Fig 2.3.2 CTS-induced Problem

III. LITERATURE SURVEY

This survey deals with various modifications done in RTS/CTS mechanism and also focuses on the drawbacks of these modified RTS/CTS mechanism.

3.1 MACA-BI

In MACA-BI [13] 4-way handshake of data transmission RTS/CTS/DATA/ACK is modified to have only 2-way handshake. The RTS packet is eliminated from handshake while CTS packet is renamed as RTR (Request-to-Receive), and now sends by receiver. Unlike original handshake this form is “receiver initiated” transmission. When any receiver is ready to receive some data, it sends RTR packet to intended sender. After receiving RTR packet successfully, sender sends the data.

Advantages:

1. This MACA-BI protocol increases network throughput in presence of hidden nodes.
2. It also helps to manage flow control, congestion control, and traffic regulation because of receiver initiated tendency.

Disadvantages:

1. This protocol is compatible with stationary network where every node knows how many packets it has to receive or how many senders are there.
2. In spite of less control packet collision, performance degradation is still an issue.

3.2 MACA – RPOLL

The basic idea of this MACA-RPOLL [12] is that whenever collision occurs at receiver node, receiver concludes that there must be more than

one intended senders. Now receiver will poll all its neighbours one by one to know whether they have any packet to send and one that has data to send is allowed to access the channel. Thus instead of letting all potential senders to go to back-off modes, receiver itself checks for sender.

Advantages:

1. This method solves the problem of unfair back-offs.
2. It gives better performance than MACA in some issues.

Disadvantages:

This protocol does not suitable for mobile networks because every node should know how many packets it has to receive or how many senders are there.

3.3 NAV Omitted

NAV Omitted [10] is a method in which a transmitter cancels needless NAV (RTS) by transmitting CRTS (Cancel RTS) to its neighbours. Fig 3.3 shows the transmission procedure of this method. In this figure, 2 which is a neighbour of sender set NAV (RTS) by overhearing RTS from the sender 1. If the sender 1 could not get CTS from its receiver, 1 sends CRTS to its neighbours in order to cancel needless NAV (RTS) of its neighbours (including 2). Overhearing of CRTS cancels its NAV (RTS) and it turns into an idle state. Fig. 3.3 shows the length of cancelled needless NAV period.

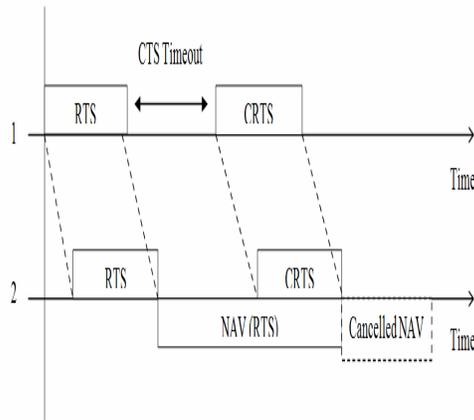


Fig 3.3 NAV Omitted

Advantages:

1. False-blocking problem due to unheard RTS and CTS packets is removed.

2. This modification improves IEEE802.11DCF throughput performance.

Disadvantage:

This mechanism works only in single hop technology.

3.4 RTS Validation

RTS validation is a method which avoids needless transmission deferment by validating the adequacy of allocated NAV. In the RTS validation, any deferring its new transmission by NAV checks DATA transmission corresponding to the NAV to carrier sensing after RTS Defer time (RTS Defer time equals CTS transmission time + 2 × SIFS periods). According to the result of carrier sensing, if no carrier is detected, the cancels the NAV and it returns to idle state. Otherwise, the node keeps its transmission deferment in order to avoid collision with ongoing transmission.

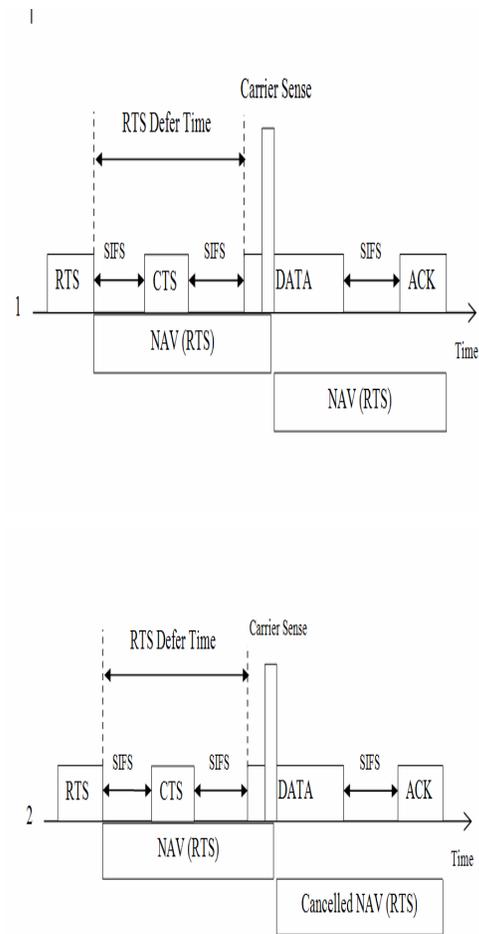


Fig 3.4 RTS Validation Mechanism

Advantages:

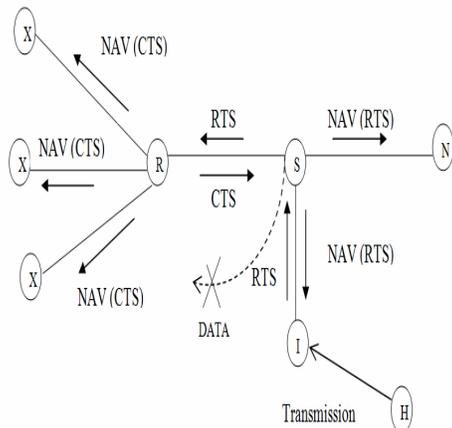
1. This mechanism prevents propagation of false blocking and also enhances the performance of RTS/CTS protocol in wireless networks.
2. This method is a back-ward compatible solution and thus can be implemented incrementally with traditional RTS/CTS mechanism.

Disadvantage:

This mechanism does not work well in multi hop topologies.

3.5 RTS/CTS + CCTS

This method [11] avoids needless NAV (CTS) caused by unheard CTS packet by introducing a new packet Cancel-CTS (CCTS). This CCTS is joined with NAV Omitting method [10] to avoid needless NAV (RTS). Thus, the problem of false blocking due to both unheard RTS and CTS packet is removed. Consider the following figure 3.5.1:



ig 3.5.1 RTS/CTS + CCTS

Let node S has a new packet destined to node R. First node S transmits RTS to node R. The RTS reaches all neighbours of node S. But, connected to hidden node H of S could not receive the RTS correctly due to collision when the node H transmits any packet in parallel with the RTS. Then, NAV (RTS) is not set at node I, and node I may interfere with a reception of CTS at S. The DATA is not transmitted from node S if the interference occurs by node I although nodes marked X in Fig defer its new transmission needlessly by receiving CTS from node R correctly.

In the following fig 3.5.2 node 2 transmits CTS to node 1, and node 1 cannot receive the CTS (due

to collision or any other interference) although node 3 receives the CTS correctly and sets NAV (CTS). After the transmission of CTS, node 2 waits for DATA time out and transmits CCTS in order to cancel needless NAV (CTS) on its neighbour nodes when node 2 could not recognize DATA transmission with carrier sensing. On receiving CCTS from node 2, node 3 cancels its NAV (CTS) and avoids needless transmission deferment induced by missing CTS.

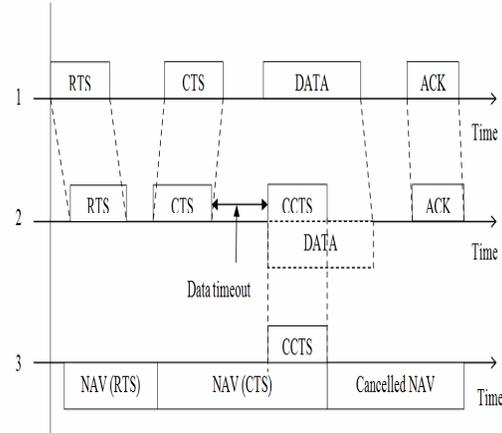


Fig 3.5.2 Cancel CTS procedure

Advantage:

This procedure solves false blocking problem due to both unheard RTS and CTS.

Disadvantage:

This mechanism degrades network performance due to additional control packets.

IV. PROPOSED MODIFICATION IN RTS/CTS MECHANISM

The proposed scheme addresses the problem of exposed terminals and also RTS-induced and CTS-induced problem. This work allows concurrent transmissions by utilizing the information heard from the neighbouring nodes during the exchange of control packets in the presence of hidden and exposed terminals. Nodes in the proposed scheme maintain the status of transmitter and receiver of itself and of its neighbouring nodes. In the proposed scheme, a hidden node can receive and an exposed node can transmit without causing collision with the ongoing transmission. It achieves successful overlapping transmissions by using a new control packet (VCTS).

V. CONCLUSION

RTS/CTS mechanism is very useful in improving the throughput and network

performance in presence of hidden nodes. But it still suffers with some additional problem like Exposed node, Masked nodes, RTS-induced and CTS-induced problem. These problems degrade the performance of RTS/CTS mechanism.

In this survey we have studied several modifications done in RTS/CTS mechanism which help to solve problems associated with it. We have also explained their advantages and disadvantages. However in our survey, we conclude that some research is still to be done to prevent the situation of hidden nodes.

REFERENCES

- [1] LAN MAN Standards Committee of the IEEE Computer Society. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. ANSI/IEEE Std. 802.11, 1999 Edition.
- [2] V.r Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: A media access protocol for wireless LANs," in *Proceedings of ACM SIGCOMM '94*. 1994, pp. 212–225, ACM.
- [3] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part 2 - the hidden node problem in carrier sense multiple access modes and the busy tone solution," *IEEE Transactions on Communications*, vol. COM-23, no. 12, pp. 1417–1433, 1975.
- [4] C .K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*, Prentice Hall, December 2001.
- [5] Z. J. Haas, J. Deng, P. Papadimitratos, and S Sajama, "Wireless ad hoc networks," in *Wiley Encyclopedia of Telecommunications*, John G. Proakis, Ed. Wiley, December 2002.
- [6] V. Kanodia, C. Li, A. Sabharwal, B. Sadeghi, and E. Knightly, "Ordered packet scheduling in wireless ad hoc networks: Mechanism and performance analysis," in *Proceedings of MOBIHOC'02*, EPFL Lausanne, Switzerland, 2002, ACM.
- [7] P. Karn, "MACA - a new channel access method for packet radio," in *ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, September 22 1990, pp. 134–140.
- [8] G. Bianchi. Performance analysis of the ieee 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, MARCH 2000.
- [9] L. Du and L. Chen. Receiver initiated network allocation vector clearing method in w lans. In *Asia-Pacific Conference on Communications*, pages 616–619, October 2005.
- [10] T. Shigeyasu, T. Hirakawa, H. Matsuno, and N. Morinaga, "Two simple modifications for improving IEEE802.11DCF throughput performance," *WCNC 2004 IEEE Wireless Communications and Networking Conference*, no. 1, March 2004 pp. 1445-1450.
- [11] Daishi, Tetsuya, Hiroshi and Norihiko, 2008. "A New MAC Protocol for Avoiding Needless Transmission Deferral Induced by Missed RTS/CTS Handshake", *IEEE*, 2008.
- [12] T. Han and L. Weijie, 2009. "An Improvement of MACA in Alleviating Hidden Terminal Problem in Ad hoc Networks".
- [13] F. Talucci, M. Gerla, L. Fratta, 1997. "MACA-BI (MACA By Invitation) A Receiver Oriented Access Protocol for Wireless Multi hop Networks".
- [14] Saikat ray, et al., "On false Blocking in RTS/CTS Based Multihop Wireless Networks" *IEEE Trans. Vehicular Technology* Vol. 56, No.2, pp 849-862 March 2007.