A Modified RTS/CTS Mechanism

Prachi Srivastava* and Dayashankar Singh**
Computer Science and Engineering, MMMEC, Gorakhpur

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. In this research paper, we are going to propose a mechanism that permits the hidden node to transmit and the exposed node to receive. The proposed mechanism also overcomes the RTS-induced and CTS-induced problem. We performed extensive simulation using NS-2 simulator. This research work intends to develop simulations to analyze the performance of the proposed solution based on the various parameters in-terms of throughput and packet delivery ratio with marginally increased in control overhead.

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

1. INTRODUCTION

Inspite 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 a node may transmit a packet using one of the following two methods: the basic access method or the RTS/CTS method. In the basic access method, a node transmits a DATA packet if it senses the channel to be idle. The receiver, upon receiving an error-free packet, returns an ACK. If the transmitting node does not get an ACK back, it enters into back-off and retransmits after the back-off period. The basic access method suffers from the well-known hidden node problem [15]. Hidden nodes cause packet collisions and thus considerably affect network performance. In order to address the issue, IEEE 802.11 supports a mechanism known as RTS/CTS handshake. 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 2 RTS/CTS mechanism is discussed with associated problem. Section 3 explains related works that describe various modifications in RTS/CTS mechanism along with drawbacks. Section 4 introduces proposed solution that modifies RTS/CTS mechanism to solve the problem associated with RTS/CTS mechanism. In section 5 simulation result is discussed. Finally section 6 concludes this work and states some possible future scope.

2. RTS/CTS MECHANISM

To reduce the collisions due to hidden nodes in CSMA 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. Any node that hears an RTS or CTS is prohibited from transmitting any signal for a period that is encoded in the duration field of the received RTS or CTS. The duration fields in RTS and CTS are set such that nodes A and B will be able to complete their communication within the prohibited period. The deferral periods are managed by a data structure called the Network

Allocation Vector (NAV) that is a counter that decreases constantly and initialized to a value stored in RTS or CTS packet. Finally, if a node does not get a response to an RTS or a DATA packet, it enters into an exponential back off mode.
For example suppose a 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. 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.

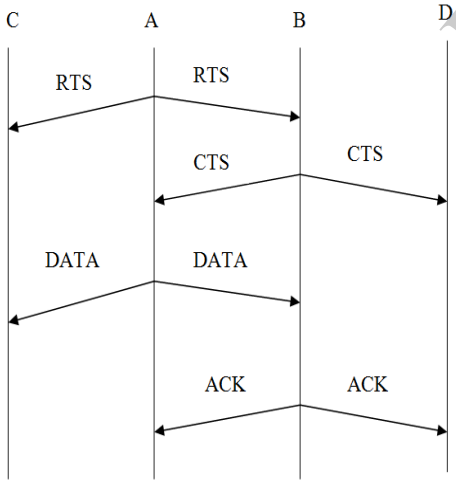

Figure 2: RTS/CTS mechanism

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.

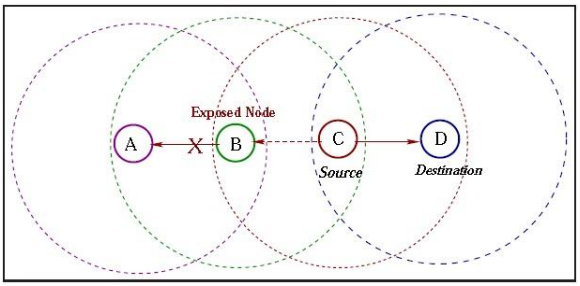

Figure 2.1 Exposed Node Problems

2.2. 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 2.2.1 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 2.2.1. 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 2.2.2 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.

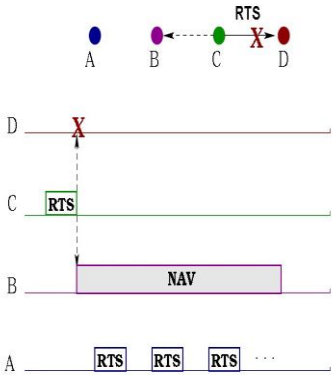

Figure 2.2.1 RTS-induced Problem

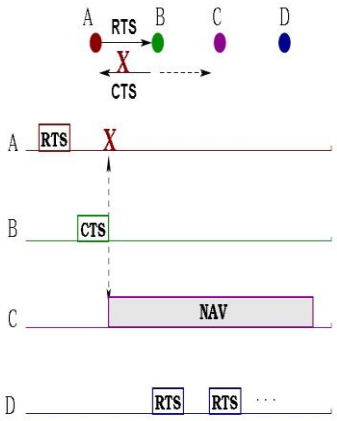

Figure 2.2.2 RTS-induced Problem

3. RELATED WORK

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

In [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. It also helps to manage flow control, congestion control, and traffic regulation because of receiver initiated tendency. The limitation of this protocol is that it only compatible with stationary network where every node knows how many packets it has to receive or how many senders are there.

In [12] when 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. This method solves the problem of unfair back-offs. 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.

In [10] transmitter cancels needless NAV (RTS) by transmitting CRTS (Cancel RTS) to its neighbours. In this a neighbour of sender set NAV (RTS) by overhearing RTS from the sender. If the sender could not get CTS from its receiver, sends CRTS to its neighbours in order to cancel needless NAV (RTS) of its neighbours. Overhearing of CRTS cancels its NAV (RTS) and it turns into an idle state. False-blocking problem due to unheard RTS and CTS packets is removed. This mechanism works only in single hop technology.

This [14] propose a method that avoids needless transmission deferment by validating the adequacy of allocated NAV. In this, 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. This method is a back-ward compatible solution and thus can be implemented incrementally with traditional RTS/CTS mechanism. This mechanism does not work well in multi hop topologies.

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. This mechanism degrades network performance due to additional control packets.

4. PRROPOSED 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).

At any point of time, the status of the transmitter and receiver of a node can be in one of the following state:

• Free: Transmitter set to Free indicates, the node is not transmitting. Receiver set to free indicates, the node is not receiving.

• Busy: Transmitter set to Busy indicates, the node is transmitting. Receiver set to busy indicates, the node is receiving.

• Unknown: Indicates that status of the transmitter and receiver of a node is not known.

Initially, each node set the status of its own transmitter and receiver as Free and neighbour nodes transmitter and receiver as Unknown. A node will set the status of its own transmitter and receiver as either Free or Busy and will never be set to Unknown. Each node in the network maintains the status of its own and neighbouring nodes transmitter and receiver as shown in figure 4.1.

Let a source S wants to transmit data to destination D. The source first checks the status of its own transmitter and destination node's receiver. If both are Free for the expected duration of transmission, then it directly transmits data to its destination. If destination node's receiver is busy it defers transmission for a busy period. If destination node's receiver is unknown it performs the following steps:

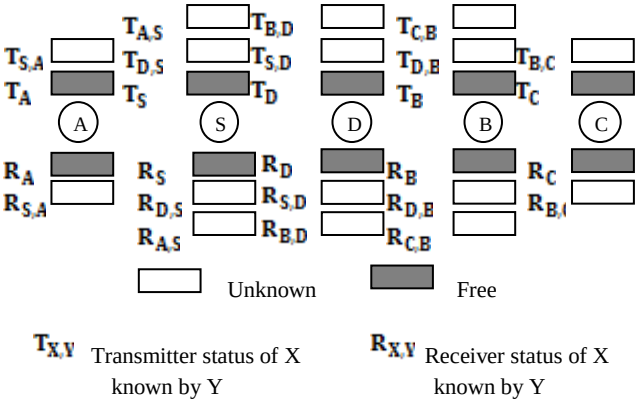

Figure 4.1: Initial Step

1. The source S sends a RTS packet to node D. The RTS packet contains the duration of data transmission. The neighbour node of S that overhears the RTS packet, starts a timer.

2. The destination node D on receiving the RTS packet performs the following actions:

• Checks the status of its own receiver and transmitter. If either or both are Busy, then node D does nothing.

• If both the receiver and transmitter of destination node is Free, then does the following actions.

(i) Set the status of source node's transmitter and receiver to Busy.

(ii) Set its own transmitter and receiver to Busy.

(iii) Transmits a CTS packet in response to RTS packet.

3. Following changes are made by the nodes other than the destination, on receiving RTS.

• Set the status of source node's transmitter and receiver to Busy.

• Set its own receiver to Busy.

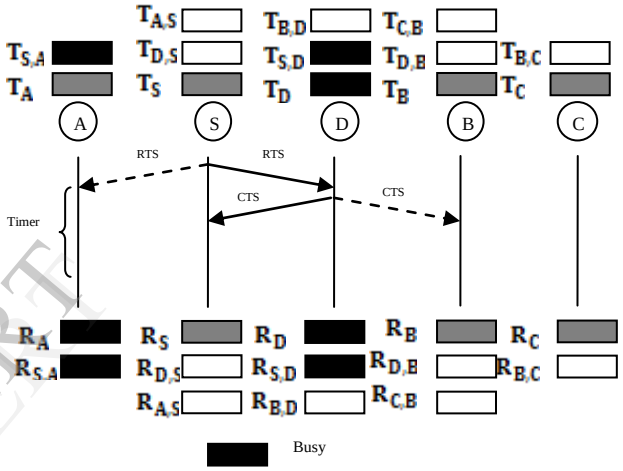

Figure 4.2: Step 1, 2 and 3

4. Following changes are made by the nodes other than the source, on receiving CTS.

• Set the status of their own transmitter to busy.

• Set the status of destination node's transmitter and receiver to Busy.

• Transmit a Validate CTS (VCTS) packet.

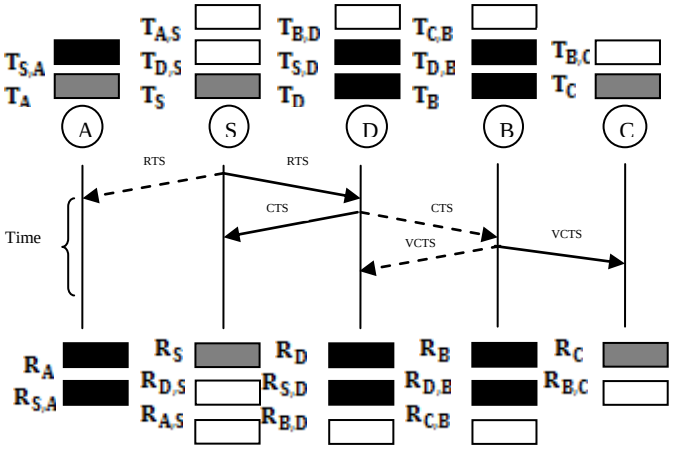

Figure 4.3: Step 4

5. Nodes including the destination make the following changes on receiving the VCTS packet.

- Set the status of the transmitter of the source of the VCTS packet to Busy.
- Set the status of the receiver of source of the VCTS packet to Free.

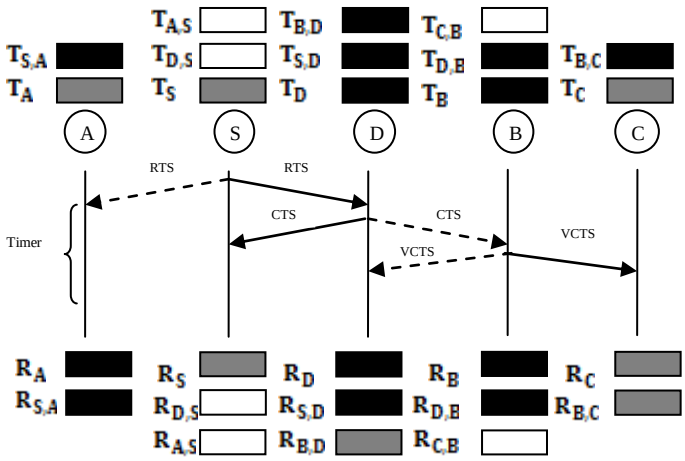

Figure 4.4: Step 5

6. The source S on receiving the CTS packet schedules the data transmission and does the following changes:

- Set the status of its own transmitter and receiver to Busy.
- Set the status of destination node's transmitter and receiver to Busy.

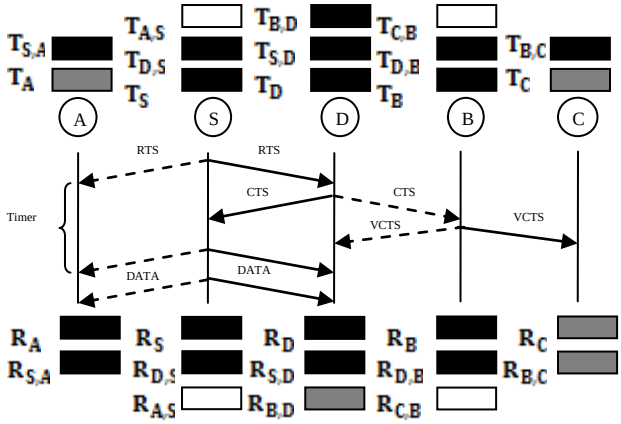

Figure 4.5: Step 6

7.

- The node D, after receiving the data packet and sends an ACK packet to acknowledge the reception of the DATA packet.
- On receiving DATA packet the neighbours of source node check the timer. If timer does not expire, stop the timer. Otherwise sets the transmitter and receiver of node S to Free and also set its own receiver to Free.

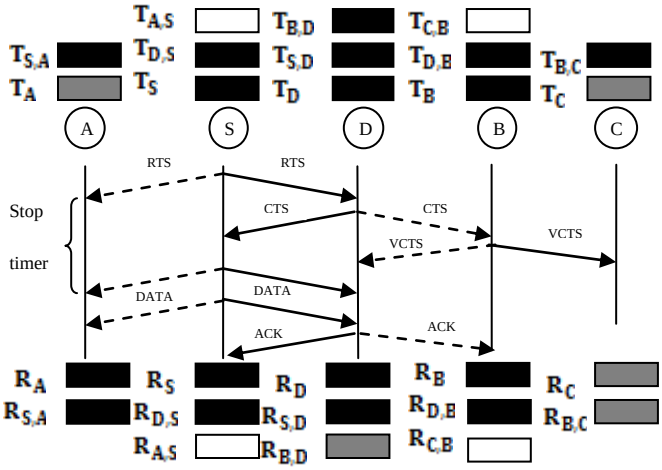

Figure 4.6: Step 7

8. After the duration of transmission is over, each node set the status of its own transmitter and receiver to free and other nodes transmitter and receiver to unknown.

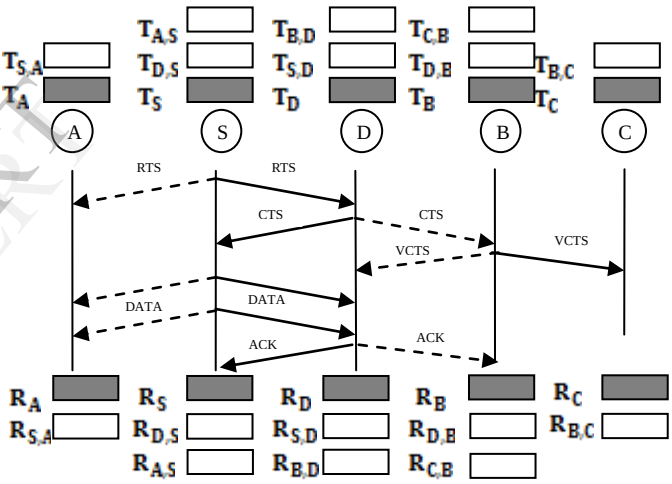

Figure 4.7: Step 8

5. SIMULATION AND RESULTS

In this section, the simulation environment and the simulation results are discussed. Simulation is done using the network simulator NS-2 [15]. To evaluate the performance of the proposed protocol, several simulations are performed. Table - 5.1 shows the simulation parameters.

Simulation Parameters:

Table 5.1 Simulation Parameter

Parameters	Values
Network size/Simulation Area	1000m * 1000m
Number of nodes	5-20
Max speed	10 m/sec
Data Packet Size	Varying from 100 - 500 bytes
Simulation time	600sec
Traffic model	CBR
Node mobility	Random
Data Rate	1Mbps

5.1 Performance Evaluation: The metrics used in evaluating the performance are:

• **Throughput**: It is defined as the amount of bits that can be transmitted in unit second. Throughput is calculated in kilo bits per second (kbps). It is observed from the figure 5.1 that the proposed method has higher throughput. This is due to the fact that in the proposed scheme, exposed nodes are allowed to transmit and hidden nodes are allowed to receive during the ongoing transmission. It is seen from Figure 5.1 that the throughput increases with the increase in number of nodes in the proposed method.

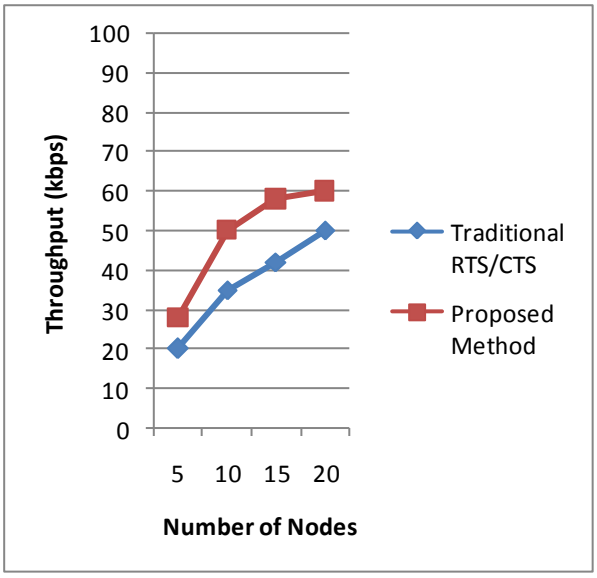

Figure 5.1: Throughput vs. Number of nodes

• **Packet Delivery Ratio:** It is the ratio of the number of data packets delivered to the destinations to the number of data packets generated by the sources. It specifies the packet loss rate, which limits the maximum throughput of the network. Figure 5.2 illustrates the packet delivery ratio vs. number of nodes. From the figure it can be seen that the packet delivery ratio is more when number of nodes are less and decreases gradually with increase in number of nodes and then saturates.

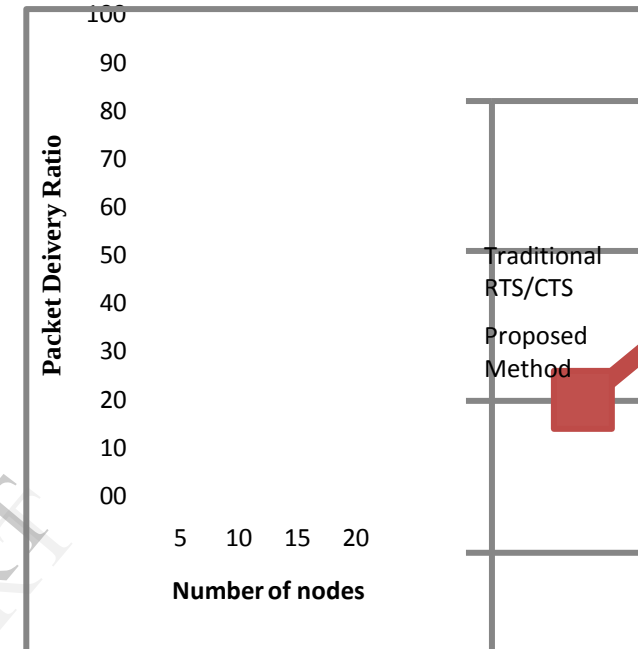

Figure 5.2: Packet Delivery Ratio vs. Number of nodes

• **Control Overhead**: The ratio between the total numbers of control packets to the data packets. The number of control packets means the number of transmitted RTS, CTS, VCTS, and ACK packets, for successfully transmitting a DATA packet from a source node to destination node. In Figure 5.3 we plot the graph for control overhead vs. number of nodes. The control overhead in the proposed method is marginally higher than the traditional method.

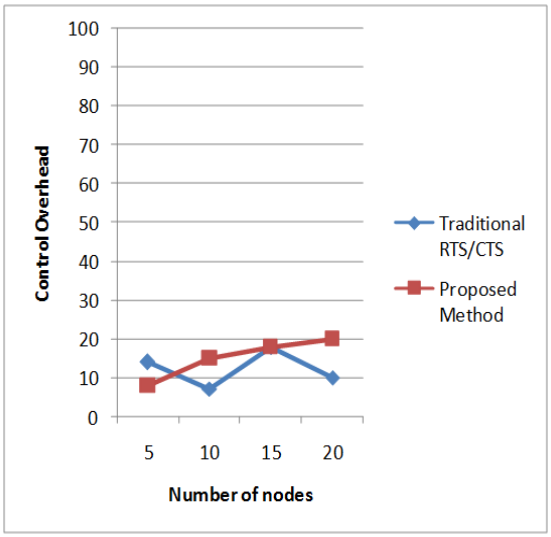

Figure 5.3: Control Overhead vs. Number of nodes

6. CONCLUSION AND FUTURE SCOPE

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, RTS-induced and CTS-induced problem. These problems degrade the performance of RTS/CTS mechanism. In our proposed modification we are avoiding the collision due to hidden terminals as well as utilizing the wasted bandwidth at these exposed and hidden nodes by allowing the exposed node to transmit and the hidden nodes to receive during data transmission at its neighbour node and also minimizing the possibility of RTS-induced and CTS-induced problems.

There are significant scopes for further improvements. As the neighbour changes dynamically, it may be costly to keep the status of the neighbouring nodes transmitter and receiver. The control overhead of the proposed modification can be minimized further by restricting the transmission of VCTS packets. These works are open for further developments of this research work.

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 Eddition.

[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 Amature 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 wlans. 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 Deferment 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, J. B. Carruthers and D. Starobinski. "RTS/CTS-Induced Congestion in Ad Hoc Wireless LANs" in 2007.

[15] The Network simulator ns-2 Project web page available at http://www.isi.edu/nsnam/ns/.

[16] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part 2 - the hidden node problem in carrier sense multiple access modesand the busy tone solution," *IEEE Transactions on Communications*, vol. COM-23, no. 12, pp. 1417–1433, 1975.