IJCSMA

N. Ramesh Babu *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 6, June- 2015, pg. 26-36 **ISSN: 2321-8363**

Flexible RTS and Concurrent Transmission Schemes for Reducing Exposed Node Problem in 802.11 WLANs

N. Ramesh Babu[1], Dr. N. Geethanjali[2]

[1] *Research Scholar, Sri Krishnadevaraya University, India. ramesh.phd.sku@gmail.com*

[2] *Associate Professor, Sri Krishnadevaraya University, India. geethanjali.sku@gmail.com*

Abstract

Hidden and exposed nodes are the problems that occur in IEEE 802.11 wireless local area networks. The hidden node problem is mitigated in such network using RTS/CTS mechanism provided by IEEE 802.11. Since then the IEEE 802.11 standard has been improved several times. The recent standard 802.11n supports multi-rate transmission. However, the problem with this is that there is significant difference between data rate and control frame rate and their coverage. Due to this, the RTS/CTS method which is meant for reducing hidden node problem actually causes exposed node problem. An exposed node is the node which is located outside the transmission range of receiver node but within the transmission range of sender node. When such nodes receive RTS from sender nodes, they have to wait until CTS and ACK from the receiver. Thus the performance of the network is deteriorated in terms of throughput. Adjusting RTS/CTS transmission rates and optimizing throughput is the area less explored in IEEE 802.11 networks. In this paper, we proposed two methods of reducing exposed nodes. First method explores RTS/CTS dynamics in terms of adjusting RTS transmission range to optimize the network throughput besides reducing exposed nodes. The second method lets nodes to identify themselves as exposed nodes based on the sequence of packets and opportunistically schedule concurrent transmissions. Empirical results through NS2 simulations revealed that the proposed methods are capable of increasing throughput by reducing exposed nodes effectively.

Keywords*:* IEEE 802.11 WLANs, Exposed Node, RTS/CTS dynamics, Concurrent transmission.

1. INTRODUCTION

IEEE 802.11 standard is widely used in mobile networks. They support ad hoc networking with direct communication among devices without the need for access points. Their access method is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). In such networks there is a problem called hidden node problem which deteriorates network performance. With respect to channel usage, the sender node does not know channel usage correctly and when the sender and other node which is outside the transmission range of sender sends packets simultaneously, it causes collisions. This is due to hidden node problem. To overcome this problem Request to Send/Clear to Send (RTS/CTS) mechanism was introduced in 802.11 standard. The hidden node problem is resolved to some extent but it caused another problem known as exposed node problem. Any node which is located outside the transmission range of sender node but within the receive range of receiver node is considered to be hidden node. Such node causes collisions in the network. Any node which is located outside the transmission range of sender node but within the transmission range of receiver node is considered to be exposed node. Figure 1 illustrates the exposed node problem in IEEE 802.11 networks.

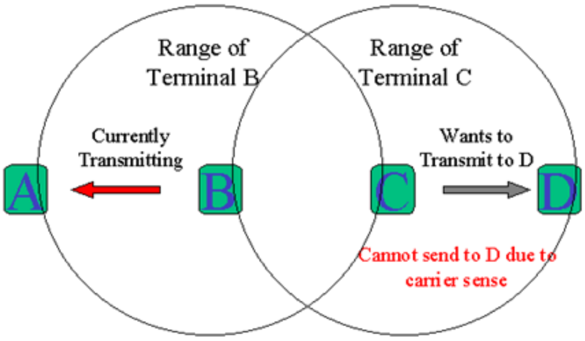


Figure 1 Exposed Node Problem in IEEE 802.11 WLANs

As shown in Figure 1, the exposed node cannot transmit data to receiver node due to carrier sense. This wait time makes the node C as exposed node. Exposed nodes cause the throughput to be decreased in such networks. According to Ganesan *et al.* [11] there is exposed node problem in IEEE 802.11 standard. A node which can hear data and RTS of the sender, according to Romuszko [15], is known as exposed node of the sender. Loton [13] proposed a tool by name wypy which could identify exposed nodes in networks. Wang *et al.* [4] explored the reasons why channel utilization is degraded in IEEE 802.11 networks due to the problem of exposed nodes.

Our contributions in this paper are as follows.

1. We proposed a method that focuses on flexible RTS transmission rate in order to reduce RTS coverage that lets exposed nodes to fall outside the rang of RTS coverage. This will help such nodes to transmit data instead of waiting for some time thus leading to increased throughput in the network.
2. We proposed an algorithm named concurrent transmission algorithm which lets nodes in the network to identify themselves as exposed nodes and initiate concurrent data transmission. This will effectively mitigate number of exposed nodes in the network leading to increase in the throughput performance of the network.
3. We made a simulation study of the proposed methods for proof of concept. Our results revealed that the two methods outperform existing method since they do have approaches for superior performance.

The remainder of the paper is structured as follows. Section 2 reviews literature on exposed node issues and prior solutions. Section 3 proposes flexible RTS scheme that can mitigate exposed nodes. Section 4 presents another method that employs concurrent transmission algorithm to reduce number of exposed nodes in the network. Section 5 presents simulation environment and the results while section 6 concludes the paper besides giving recommendations for future work

2. RELATED WORKS

This section reviews literature on exposed node problem in IEEE 802.11 and its related works. Borgo *et al.* [9] investigated the problems with effects of hidden terminals in IEEE 802.11b networks and specified the importance of RTS/CTS to overcome the problem. Zubow and Sombrutzki [8] explored the adjacent channel interference or channel orthogonality in IEEE 802.11n networks. Especially they focused on the adverse effects of the Adjacent Channel Interference (ACI) which is one of the forms of exposed node problems. They concluded that 802.11 standard is not appropriate for multi-channel routing protocols. Radunovic *et al.* [14] proposed a novel mechanism known as self-interference cancellation to reduce the hidden node and exposed node problems in distributed wireless networks. Jayasuriya *et al.* [18] investigated the problems of hidden and exposed nodes in wireless networks. They concluded that RTS/CTS solution solves the problem of hidden nodes but causes exposed nodes that need to be resolved.

Shukla *et al*. [1] proposed a method to handle exposed node problem. According to their method, the exposed node itself will be able to know that it is an exposed node. It is achieved by receiving RTS which was not for it and at the same time not receiving CTS while receiving the data from the sender of RTS. Thus the node can send data in parallel with the sender node which will improve throughput. Later on Kim and Shim in [10] improved the method explored in [1] by incorporating interference range and the transmission of data from exposed node is synchronized with the sender node which transmits data. Afterwards Nishide *et al*. [3] and Mittal and Belding [12] tried a new method that considers maintaining a database which contains information of all nodes including the position of exposed nodes. Then the method exploits the operations specified in [4] and [5] to exploit the possible transmission of data without having exposed node problem and thus improve the throughput of the network. Jiang and Liew [2] proposed a new method known as Selective Disregard of NAVs (SDN) which let the nodes to ignore carrier sense selectively thus reducing the possible exposed nodes in IEEE 802.11 networks. Further studies made in [5], [6], [7] and [17] used different transmission rates of RTS/CTS frames in order to reduce exposed node problems. Our proposed method is in similar lines which explores the flexible dynamics of RTS/CTS frames in order to identify exposed nodes in real time and let them transfer data in parallel with the actual sender node whose carrier sense is known to the exposed node.

3. PROBLEMS WITH RTS/CTS METHOD

As IEEE 802.11 is vulnerable to hidden node problems, the 802.11 is enhanced several times in order to improve the wireless communications. Towards this end, RTS/CTS was proposed to solve hidden node problem. Though it was able to solve hidden node problem, it caused another problem known as exposed node problem. Exposed node is the node which will not be able to transmit data to its destination node even though the channel is free as it follows carrier sense of other sender node and waits for some time to send data unnecessarily. This problem leads to the degradation of throughput in wireless networks. This problem is illustrated in Figure 2 and the problem is described with four nodes such as exposed node, sender node, receiver node and hidden node.

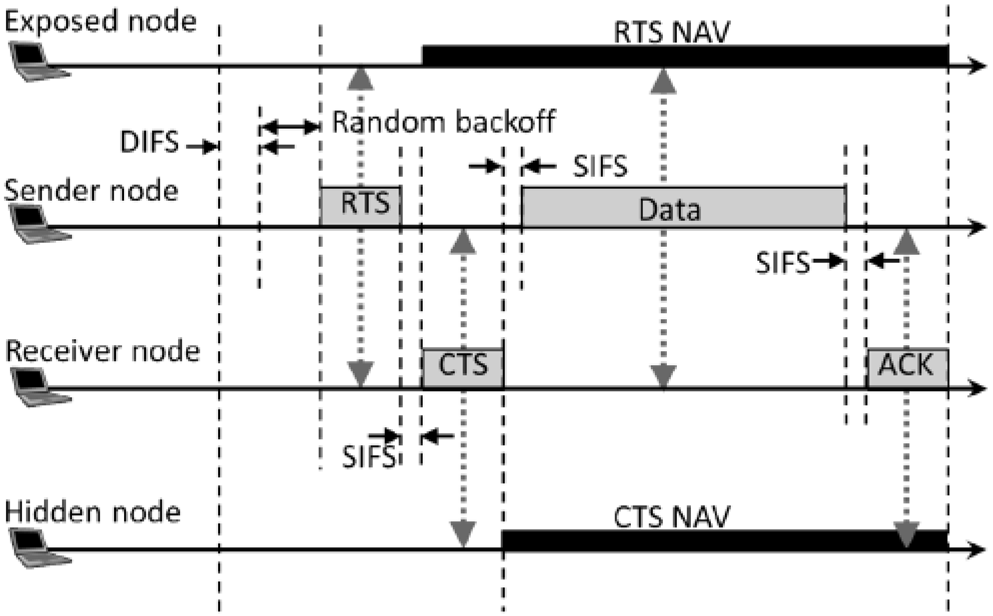


Figure 2 RTS/CTS Mechanism of IEEE 802.11 Standard

From the above figure it is understood that there are four nodes involved in the network. The nodes are exposed node, sender node, receiver node and hidden node. It shows how the nodes are involved in communications. The figure illustrates the hidden node problem and exposed node problem. A sender node sends RTS frame to receiver node. The RTS is also received by the exposed node and waits for some time without transmitting data due to carrier sense that indicates that the channel is busy. However the channel is not really busy. For this reason the throughput of the network is reduced. The following are the steps involved in RTC/CTS method.

1. After performing carrier sense, a sender node sends RTS. The sender node waits to know whether channel is free. It also waits DIFS period and also random back off period before actually transferring data. At this period, the exposed nodes need to wait for NAV period.
2. After SIFS period, the receiver node sends CTS after receiving RTS from sender node. At this period CTS is received by hidden nodes also. The hidden nodes are to wait for NAV period holding transmissions as done by all nodes who receive CTS.
3. Afterwards, the sender node sends data frame after SIFS period to receiver once it receives CTS.
4. The receiver node receives data frame and send ACK back to the sender node after SIFS time.

In the early version of IEEE 802.11, this mechanism was introduced. It could solve the hidden node problem. However, it caused the exposed node problem. In this paper we proposed a method that makes flexible use of RTS/CTS frames in order to ensure that the exposed nodes do not hold their transmissions unnecessarily and utilize the channel to transmit data.

4. PROPOSED METHODOLOGIES

4.1 MITIGATING EXPOSED NODES USING FLEXIBLE RTS/CTS TRANSMISSION

There are many approaches to solve hidden node problem as explored in literature. The proposed methodology solves this problem with flexible transmission rates of RTS/CTS frames. We explored the dynamics of identifying exposed nodes and compute the adjustments required by the RTS/CTS frames in order to ensure that the exposed nodes do not waste time unnecessarily. Thus the exposed nodes send data to destination in parallel with the actual sender node that sent the RTS frame. Therefore the throughput of the network is increased. First of all, we describe the identification of exposed nodes. For a given node, all exposed nodes are found. Consider figure 2.

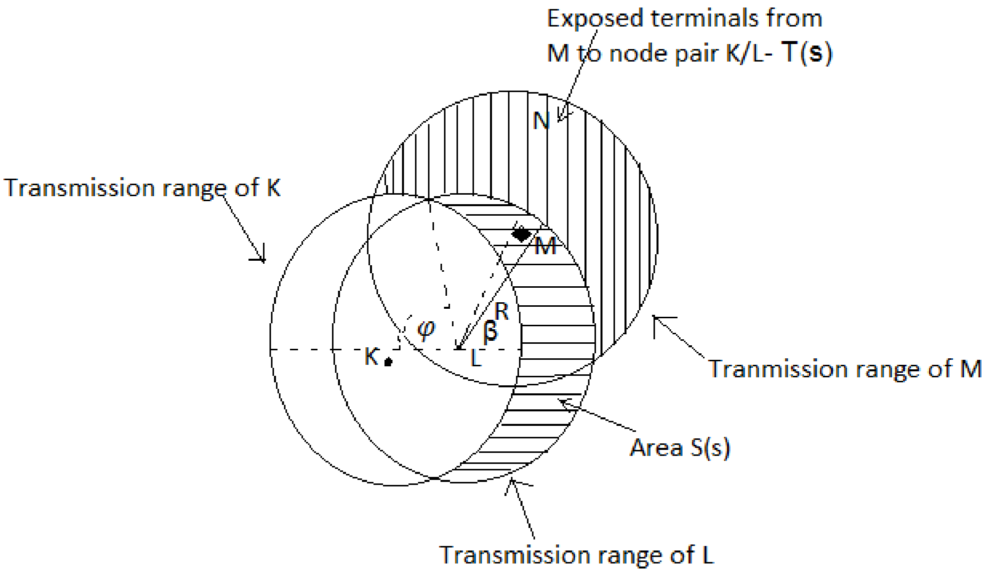


Figure 3: Identifying the Exposed Nodes

As shown in Figure 2, from M to node pair K/L-T(s). It also shows transmission range of K, transmission range of M, area S(s), transmission range of L. The following equation represents the dynamics illustrated in Figure 2.

$$T(s,t,\beta) = \pi R^2 - 2R^2 arccos\left(\frac{t}{2R}\right) + \frac{t}{2}\sqrt{4R^2 - t^2}$$

If the M is located outside the circle with respect to T, the area T can be expressed as follows.

$$\pi R^2 - 2R^2 arccos\left(\frac{t}{2R}\right) + \frac{t}{2}\sqrt{4R^2 - t^2} - T_3(s,t,\beta)$$

By integrating over T, S regions it is possible to fid number of exposed terminals as follows.

$$\frac{2}{R^2}\int_0^K s\int_0^{\pi-\varphi}\int_{r_1}^K 2T(s,t,\beta)\sigma^2 tdtd\beta ds$$

Where

R – Transmission/reception range of the nodes

σ - Node density of the network

φ = arccos($\frac{s}{2R}$)

r$_n$=$\sqrt{R^2 - s^2 sin\beta} - scos\beta$

$$T(s,t,\beta) = \pi R^2 - 2R^2 arccos\left(\frac{t}{2R}\right) + \frac{t}{2}\sqrt{4R^2 - t^2} - T_3(s,t,\beta)$$

=T$_1$(s,r,β)

Or

$$T(s,t,\beta) = \pi R^2 - 2R^2 arccos\left(\frac{t}{2R}\right) + \frac{t}{2}\sqrt{4R^2 - t^2} - T_3(s,t,\beta)$$

=T$_2$(s,r,β)

Depending on the position of M.

O>1.03$^{\sigma^2 R^4}$

$\frac{\sigma t d\beta dt}{\sigma\pi R^2}$

Then the average probability of this event is

P$_{av}$=$\frac{2}{R^2}\int_0^K 2s\int_0^{\pi-\varphi}\int_{r_1}^K \frac{t}{\pi R^2} dtd\beta ds$

=$\frac{2}{\pi R^6}\int_0^R s\left(S(s^3 - sR^2) + 2R^4 arctan\left(\frac{sS}{2R^2 - s^2}\right)\right) ds$

=0.28

Where r$_n$, φ and S are as defined before.

Once exposed nodes are found for each node, it is possible to adjust flexible frame rates for RTS/CTS so as to ensure that the Exposed nodes do not wait unnecessarily thus improving throughput of the network. By increasing RTS transmission rate, it is possible to decrease RTS coverage. The RTS transmission rate can be increased to the rate of data frame so as to reach maximum rate. With higher transmission rate, the effective transmission range becomes shorter. As a result some of the exposed nodes fall short of the RTS range and therefore they need not to hold their transmissions. Thus the number of exposed nodes is effectively reduced besides increasing the overall throughput of the network.

4.2 MITIGATING EXPOSED NODES USING CONCURRENT TRANSMISSION ALGORITHM

This is the second approach we propose in this paper to mitigate exposed nodes. The nodes in the WLAN can identify themselves as exposed nodes when they are subjected to that situation and opportunistically schedule concurrent transmission as and when required.

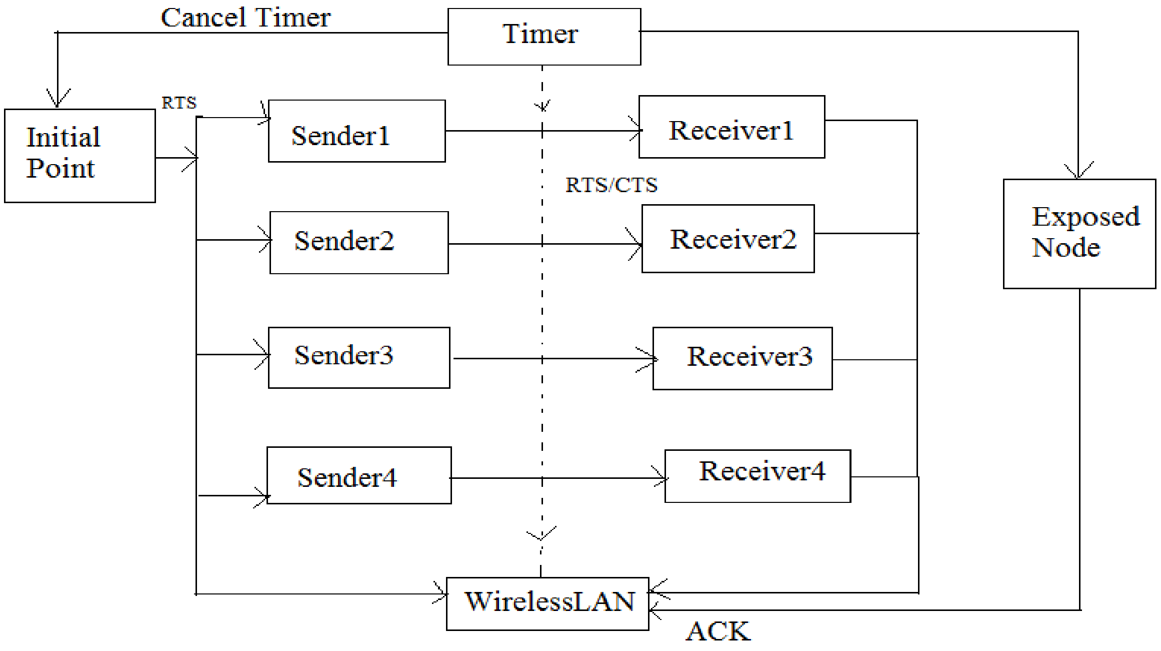
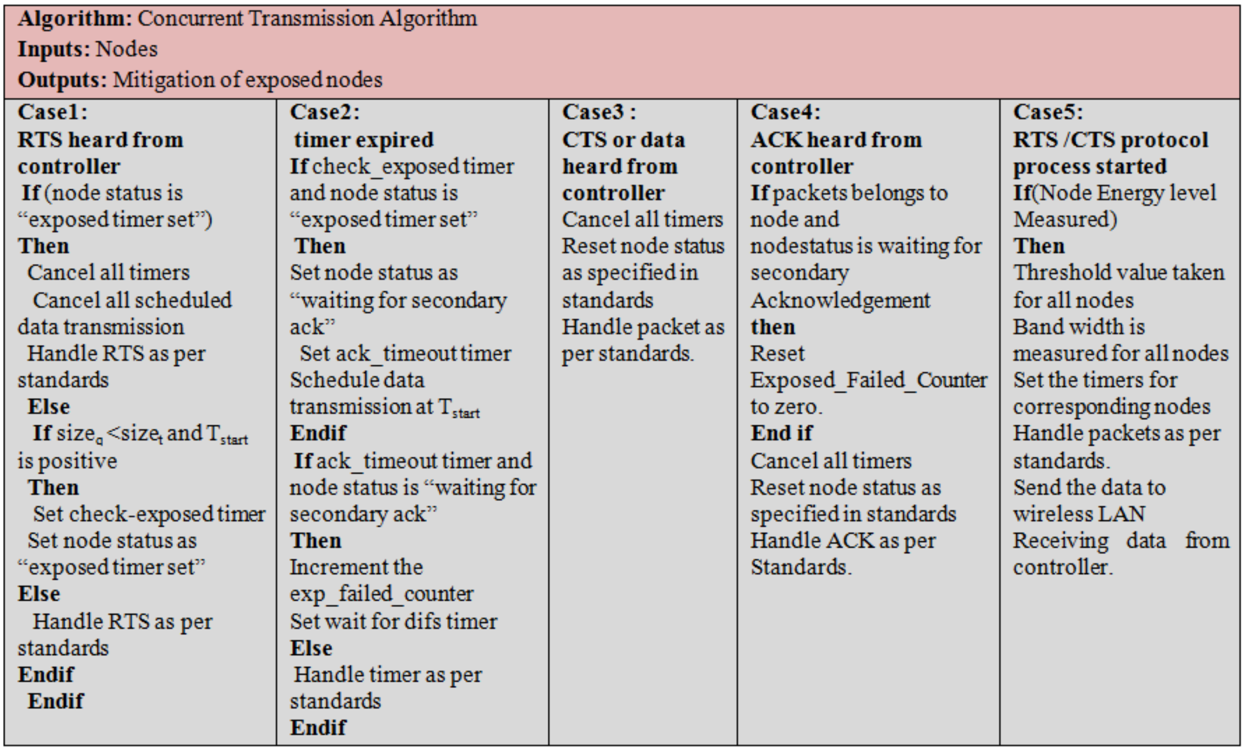


Figure 4: Overview of the concurrent transmission algorithm

As shown in Figure 3, the nodes in the network perform concurrent transmissions whenever possible thus reducing exposed node problem. It also reduces loss of throughput caused by the exposed node problem. The conceptual flow of the proposed scheme is presented as concurrent transmission algorithm as shown in Figure 4.



Algorithm: Concurrent Transmission Algorithm
Inputs: Nodes
Outputs: Mitigation of exposed nodes

Case1: **RTS heard from controller**	**Case2:** **timer expired**	**Case3 :** **CTS or data heard from controller**	**Case4:** **ACK heard from controller**	**Case5:** **RTS /CTS protocol process started**
If (node status is "exposed timer set") **Then** Cancel all timers Cancel all scheduled data transmission Handle RTS as per standards **Else** **If** size$_q$ <size$_t$ and T$_{start}$ is positive **Then** Set check-exposed timer Set node status as "exposed timer set" **Else** Handle RTS as per standards **Endif** **Endif**	**If** check_exposed timer and node status is "exposed timer set" **Then** Set node status as "waiting for secondary ack" Set ack_timeout timer Schedule data transmission at T$_{start}$ **Endif** **If** ack_timeout timer and node status is "waiting for secondary ack" **Then** Increment the exp_failed_counter Set wait for difs timer **Else** Handle timer as per standards **Endif**	Cancel all timers Reset node status as specified in standards Handle packet as per standards.	**If** packets belongs to node and nodestatus is waiting for secondary Acknowledgement **then** Reset Exposed_Failed_Counter to zero. **End if** Cancel all timers Reset node status as specified in standards Handle ACK as per Standards.	**If**(Node Energy level Measured) **Then** Threshold value taken for all nodes Band width is measured for all nodes Set the timers for corresponding nodes Handle packets as per standards. Send the data to wireless LAN Receiving data from controller.

Figure 5: Concurrent Transmission Algorithm

The algorithm has five cases which are meant for ensuring that the exposed nodes are mitigated and the overall performance of network is increased. Case 1 is executed when RTS is heard from controller. The second case is executed when timer is expired. Case 3 is executed when CTS or data heard from controller. Case 4 is executed when ACK is heard from controller while case 5 is executed when RTS/CTS protocol process is started. The aim of the protocol is to ensure that nodes in the network opportunistically explore the possibilities of scheduling transmissions concurrently. With the help of this algorithm, the nodes can identify themselves as exposed nodes based on the sequence of packets heard by them. When a node hears RTS followed by data from same node in the given time, that node considers itself as exposed node and initiates parallel transmission of data without participating RTS/CTS exchange. The simulation results of the concurrent transmission algorithm can be found in the ensuing section.

5. EXPERIMENTAL RESULTS

This section provides the experimental environment and results of the experiments made via NS2 simulations. The results reveal that the proposed system is able to identify exposed nodes and have some flexible RTS/CTS mechanism in order to reduce number of exposed nodes and thus increase the overall throughput of the network. By applying the proposed system to IEEE 802.11 network it is possible to overcome the problems of the RTS/CTS provided by original 802.11 standard. The RTS transmission range and RTS coverage are recorded as the proposed scheme is implemented to reduce exposed nodes. The results are as follows.

Table 1: Environment used for Simulation

PARAMETER	**SPECIFICATION**
Simulation tools used	Network Simulator 2
Simulation time	60 sec, 120 sec, 200 sec

Number of nodes	30
Transmission range	150m
Maximum speed	CBR [constant bit rate] [20]
Application traffic	512bytes
Packet size	100 bytes
Routing Protocol	AODV
Number of runs	40
Threshold value	80

Table 2: Dynamics of RTS/CTS coverage

RTS Transmission Rate	RTS Coverage
2Mbps	85m
5Mbps	60m
8Mbps	38m
10Mbps	32m
13Mbps	25m
18Mbps	25m
20Mbps	12m

As shown in Table 2, the RTS coverage is decreased gradually as the RTS transmission range is increased. When coverage is decreased, it is possible that the nodes which are said to be possible exposed nodes are out of the coverage range and they are no longer exposed nodes. Thus the flexible adjustment in RTS transmission range can reduce the number of exposed nodes in the given network. The simulation results pertaining to performance of the network due to the proposed schemes for mitigating exposed nodes are as shown in Table 3.

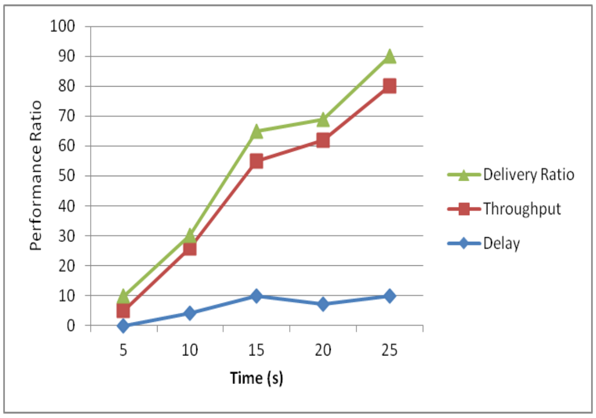


Figure 6: Performance analysis of Flexible RTS Scheme

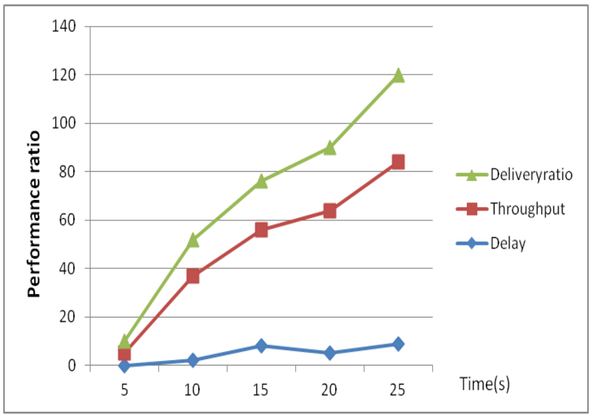


Figure 7: Performance analysis of concurrent Transmission scheme

Consider the figure 6 & 7, the horizontal axis represents time taken while the vertical axis represents performance ratio with respect to delay, throughput and delivery ratio.

The results of the proposed schemes such as flexible RTS transmission rate and concurrent transmission algorithm are reflected in Fig.6 and Fig.7 respectively. From the above figures it is evident that the proposed schemes improve performance in terms of delay, throughput, and packet delivery ratio. The throughput of the network is increased in the proposed schemes as they are able to reduce exposed nodes. The proposed schemes overcome this problem by reducing exposed nodes through flexible RTS transmission rate and through concurrent transmission respectively.

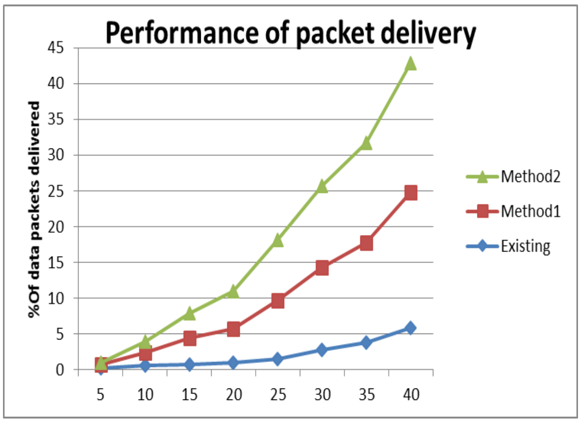


Figure 9: Comparison of Packet delivery Ratio

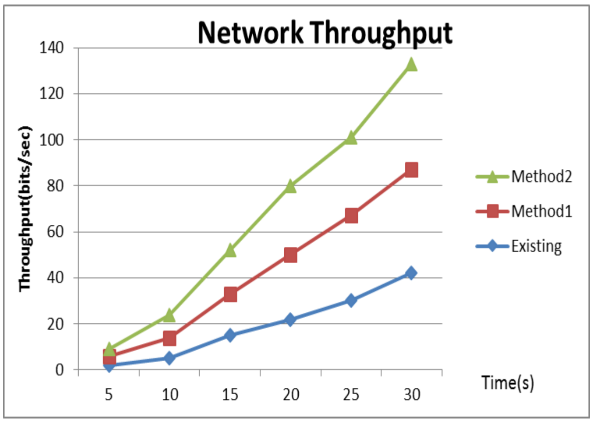


Figure 8: Comparison of Throughput

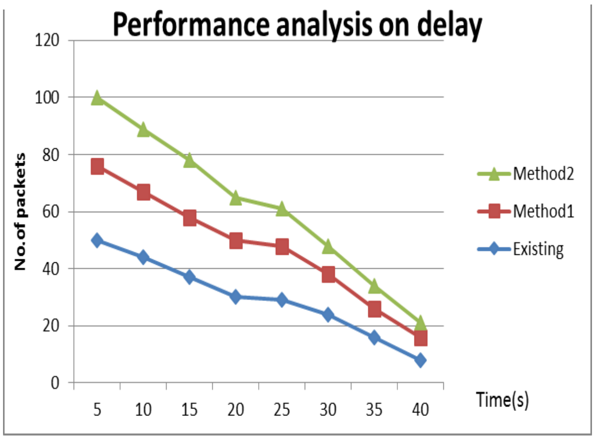


Figure 10: Comparison of delay

It is evident from the figures 8, 9 & 10 that the proposed systems has shown improved throughput performance, packet delivery ratio and decreased the delay of packets in the network. Consider the method1 in which it is capable of identifying the exposed nodes and applies the flexible RTS/CTS dynamics. It does mean that the transmission rate of RTS is increased so that its coverage is effectively reduced. This will result in many exposed nodes falling out of the range of RTS so that they will not hold transmission of data unnecessarily. This leads to the increased throughput in the proposed system. In method-2 by using the concurrent algorithm, the nodes can identify themselves as exposed nodes based on the sequence of packets heard by them and initiates parallel transmission of data without participating RTS/CTS exchange. Thus the exposed nodes are reduced drastically leading to the overall throughput performance of the network.

6. CONCLUSIONS AND RECOMMENDATIONS

In this paper, we explored the problem of exposed nodes in IEEE 802.11 networks. The initial 802.11 standard caused hidden node problem that caused collisions. Many collision recovery algorithms came into existence. Our previous paper threw light into a hybrid methodology that could overcome the hidden node problem using a retransmission scheme. In IEEE 802.11 standards RTS/CTS concept was introduced to overcome the problem of hidden nodes. However, it caused another problem known as exposed node problem. In this paper our focus is on the exposed node problem. We believed that the adjustment in transmission rate of RTS/CTS can have its impact on the throughput of the network. Towards this end our proposed solution finds the exposed nodes for each and every node. This knowledge helps in making well informed decisions. Later our approach considers making flexible adjustments in RTS transmission rate so as to influence the range of RTS. When RTS transmission is rate is increased to maximum, it results in shorter range of RTS. As a resource many exposed nodes fall out of the range of RTS. Thus they do not hold their transmissions unnecessarily. This will increase the overall throughput performance of the network. Our empirical study with NS2 simulations reveals the same. In future we would like to improve our methodology further in order to improve the performance of IEEE 802.11 networks further.

References

[1] D. Shukla, L. Chandran-Wadia, and S. Iyer, “Mitigating the exposed node problem in IEEE 802.11 ad hoc networks,” in Proceedings of the 12th International Conference on Computer Communications and Networks, Dallas, TX, 2003, pp. 157-162.

[2] L. B. Jiang and S. C. Liew, “improving throughput and fairness by reducing exposed and hidden nodes in 802.11 networks,” IEEE Transactions on Mobile Computing, vol. 7, no. 1, pp. 34-49, 2008.

[3] K. Nishide, H. Kubo, R. Shinkuma, and T. Takahashi, “Detecting hidden and exposed terminal problems in densely deployed wireless networks,” IEEE Transactions on Wireless Communications, vol. 11, no. 11, pp. 3841-3849, 2012.

[4] Guoqiang Wang, Yongchang Ji, Dan C. Marinescu. (2005). A Simulation Study of Location- and Power-aware Wireless Networks with Asymmetric Links. *ISSN*, p1-18.

[5] G. Anastasi, E. Borgia, M. Conti, and E. Gregori, “IEEE 802.11b ad hoc networks: performance measurements,”Cluster Computing, vol. 8, no. 2-3, pp. 135-145, 2005.

[6] X. Yang and N. H. Vaidya, “On physical carrier sensing in wireless ad hoc networks,” in Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, 2005, pp. 2525-2535.

[7] M. Borgo, A. Zanella, P. Bisaglia, and S. Merlin, “Analysis of the hidden terminal effect in multi-rate IEEE 802.11b networks,” in Proceedings of the International Symposium on Wireless Personal Multimedia Communication, Abano Terme (Padova), Italy, 2004, pp. 6-10.

[8] Anatolij Zubow and Robert Sombrutzki. (2004). Reinvestigating Channel Orthogonality - Adjacent Channel Interference in IEEE 802.11n Networks. *Academy of Management Executive*, p1-18.

[9] Mauro Borgo, Andrea Zanella, Paola Bisaglia, Simone Merlin. (1999). Analysis of the hidden terminal effect in multi-rate IEEE 802.11b networks. *Department of Computer Science*, p1-18.

[10] D. Kim and E. Shim, “P-MAC: parallel transmissions in IEEE 802.11 based ad hoc networks with interference ranges,” in Proceedings of the International Conference on Information Networking, Convergence in Broadband andMobile Networking, Jeju Island, Korea, 2005, pp. 735-744.

[11] Deepak Ganesan y, Deborah Estrin. (2001). Complex Behavior at Scale: An Experimental Study of Low-Power Wireless Sensor Networks.*Department of Computer Science*, p1-6.

[12] K. Mittal and E. M. Belding, “RTSS/CTSS: mitigation of exposed terminals in static 802.11-based mesh network,” in Proceedings of the 2nd IEEE Workshop on Wireless Mesh Networks, Reston, VA, 2006, pp. 3-12.

[13] Reza M. E. Lotun. (2004). wypy: An Extensible, Online Interference Detection Tool for Wireless Networks. *The Faculty of Graduate Studies*. n.d (n.d), p1-16.

[14] Bozidar Radunovic, Dinan Gunawardena, Alexandre Proutiere,. (2009). Efficiency and Fairness in Distributed Wireless Networks through Self-interference Cancellation and Scheduling. *Microsoft Research,Cambridge, UK,* p1-18.

[15] Sylwia Van den Heuvel - Romaszko, Chris Blondia. (2001). A survey of MAC protocols for Ad Hoc networks and IEEE 802.11. *Department of Computer Science*, p1-18.

[16] Aruna Jayasuriya, Sylvie Perreau, Arek Dadej, Steven Gordon, “Hidden vs. Exposed Terminal Problem in Ad hoc Networks”, p1-8.

[17] Akihisa Matoba, Masaki Hanada, Hidehiro Kanemitsu, and Moo Wan Kim, “Asymmetric RTS/CTS for Exposed Node Reduction in IEEE 802.11 Ad Hoc Networks”, JCSE, Vol. 8, No. 2, p107-118.

A Brief Authors Biography

N. Ramesh Babu – Mr. N. Ramesh Babu obtained his Master of Science in Computer Science degree at Sri Krishnadevaraya Unversity, Ananthapuramu, India and he is pursuing Ph.D in Computer Science & Technology from Sri Krishnadevaraya University. Anantapuramu, India. His research interest includes Computer Networks, Cloud Computing and Programming languages.

Dr. N. Geethanjali – Dr. N. Geethanjali received her PhD Degree from Sri Krishanadevaraya University. Andhra Pradesh, India. Currently she is an Associate Professor Computer Science & Technology, Sri Krishanadevaraya University. Andhra Pradesh, India. She is a Professional Member of ACM. Her research interest includes Computer Networks, Cloud Computing, Software Engineering, Programming languages and Data Mining