
Performance Analysis and Mitigation of Hidden and Exposed Terminal Problem in MANETs

(IJSNT) International Journal of
Communication Systems and Network
Technologies

ISSN Number: 2053-6283

Volume 2, Issue No. 2, 49–57

©The Author(s) 2013

<https://journals.mirlabs.in/index.php/ijcsnt>

DOI-10.18486/ijcsnt/2.2.021



Sanjay Singh Kushwah¹, Sarita Singh Bhadauria², Geetam S Tomar³

Abstract

Ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any network infrastructure or centralized administration. In this work, an attempt has been made to mitigate hidden terminal and exposed terminal problems of MAC layer in MANET after the performance analysis of network on the basis of previous works. The performance differentials are also analyzed on high mobility of ad hoc networks.

Keywords

Ad Hoc Network, Hidden, Exposed, Deafness

Received: 05 May 2013; **Revised:** 10 July 2013; **Accepted:** 20 August 2013;

Published: 31 August 2013;

¹Gwalior Engineering College, Gwalior, Madhya Pradesh, India.

²Madhav Institute of Technology & Sc., Gwalior, Madhya Pradesh, India.

³Machine Intelligence Research Labs, Gwalior, Madhya Pradesh, India.

Corresponding author:

Email: sanjayskushwah@rediffmail.com



© 2013 by Sanjay Singh Kushwah, Sarita Singh Bhadauria and Geetam S Tomar Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license, (<http://creativecommons.org/licenses/by/4.0/>). This work is licensed under a Creative Commons Attribution 4.0 International License

Introduction

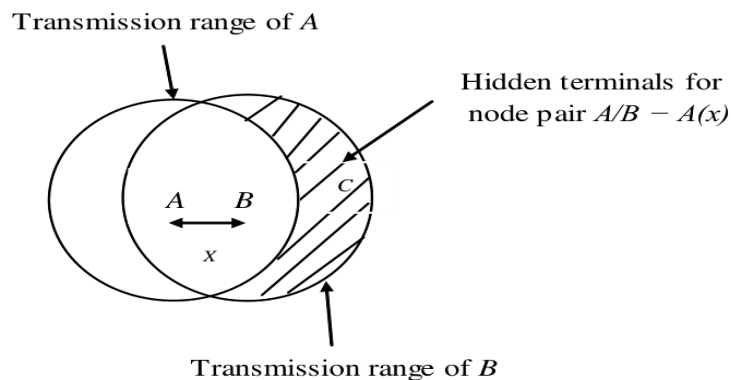
The ad hoc networks are gaining attention of researchers and industry due to its uniqueness to provide connectivity and communication. However, due to use of directional antennas for performance enhancement there have been some problems, which need to be eliminated for gaining maximum performance of the network. There are two major problems due to use of DMAC, which are hidden terminal and exposed terminal problems. The hidden and exposed terminal problems degrade the throughput of wireless networks due to collisions and wasting transmission opportunity respectively^[1]. In existing literature, a handshake mechanism called RTS/CTS to mitigate the hidden terminal problem has been used. However, RTS/CTS induces the exposed terminal problem other problems like false blocking, where some nodes that heard the RTS/CTS exchange refrain from transmission even though they would not have interfered with any ongoing transmission in ad hoc networks^[2].

IEEE 802.11 is a standard for WLANs^[3], deals with the physical and MAC layers in WLANs. Under IEEE 802.11 mobile terminals can operate in two modes; Infrastructure mode and ad hoc mode. In infrastructure mode mobile terminals can communicate with one or more access points are connected to a WLAN and when mobile terminals can communicate directly with each other without using an access points is ad hoc mode. In the IEEE 802.11 MAC, the distributed coordination function (DCF) coordinates medium access in ad hoc networks^[4]. A request to send (RTS) / clear to send (CTS) handshake precedes data communication and the following acknowledgement (ACK) in DCF, this hand shaking is termed as two way handshaking also^[5]. Two forms of carrier sensing s used in DCF as physical (by listening to the wireless shared medium) and virtual. Nodes located in the vicinity of communicating nodes, which overhear either of these control packets, must themselves defer transmission for the proposed duration. This is known as virtual carrier sensing, uses the duration field which is included in the header of RTS and CTS. This duration field is utilized to set a station's network allocation vector (NAV), which indicates the remaining time the medium is busy with the ongoing transmission. Nodes update their NAVs whenever they receive a packet using the duration information. IEEE 802.11 almost overcomes the hidden terminal problem^[2], but it induces the exposed terminal problem. Detailed description is presented of hidden and exposed terminal problem in the next section.

Hidden and Exposed Terminals Problem

The hidden terminal problem found in contention based protocols, such as ALOHA, slotted ALOHA, CSMA and IEEE802.11 etc. Two nodes are hidden terminal from one other (not within the direct transmission range of the sender) when both attempt to send information to the same receiving node. Collision occurs when both nodes transmit packets at the same time^[2,6]. This problem is depicted by Figure 1.

In Figure 1, node A wants to transmit to node B located at a distance x from A. By only sensing the medium, node A will not be able to hear transmissions by any node C in the dashed area denoted by $A(x)$. Node A will start transmitting, leading to collisions at node B. This is hidden terminal problem, where the hidden nodes are located in the area $A(x)$. The handshake (RTS/CTS) mechanism was introduced to wireless MAC layers to reduce the hidden terminal problem. However, this mechanism introduces a new problem referred the exposed terminal problem. Overhearing a data transmission from neighboring nodes can inhibit one node from transmitting to other nodes. This is known as the exposed terminal / node problem. In this problem, a node is a node in range of the transmitter, but out of range of the receiver.



78

Figure 1. The hidden terminal problem

Figure 2 is shown exposed node problem. In the example of exposed node problem, node A sends an RTS and waits for B to send a CTS. Suppose a node D located in area Y (x) wants to transmit data to node C located in area X(x), and D transmits a RTS to C just before A sends the RTS to B. After receiving the RTS from D, C transmits a CTS. This CTS is heard by B upon which B will enter a backoff period preventing B from sending the CTS to A. It is falsely concludes that it cannot transmit to C, even though it can do so simultaneously. Thus, because of B's exposed location to A, it defers its transmission even when it need not. The node in the region Y(x) is the exposed terminals for the node pair A/B.

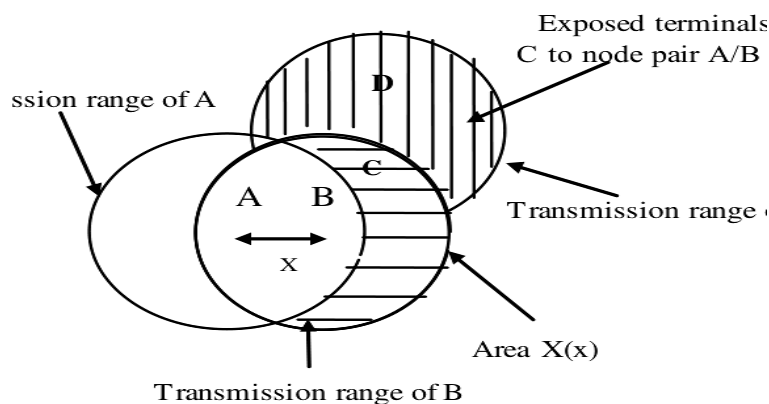


Figure 2. The exposed terminal problem

The hidden and exposed terminal problems significantly reduce the throughput of a network when the traffic load is high. It is therefore desirable that the MAC protocol be free from the hidden and exposed terminal problems. Performance evaluation is presented in next section.

Performance Evaluation

The Qualnet^[6] simulator is used to evaluate the performance of hidden terminal and exposed problem on high mobility for MANETs. Simulations are run for duration of 300s. The simulations parameters are given in the Table 1.

Table 1. Parameters Used during Simulations

Parameters	Value
Simulation Area	1500 x 1500
Simulation time	600 Secs.
Internet Protocol	IPV4
Mobility model	Random waypoint
Physical Layer	802.11b Radio
MAC	802.11
Transmission Power at 1 Mbps	15 dbm

The performance of the network was evaluated at variation of speed of nodes at 10ms^{-1} to 40ms^{-1} . However total number of nodes is 3 used in simulation and packet sizes is 512 bytes.

Figure 1 and Figure 2 shows the MAC performance in terms of broadcast sent, broadcast received, RTS sent, CTS received and drop due to retransmit limit using AODV and DSR respectively at high speed considered 40ms^{-1} . Packet length is taken variable^[7].

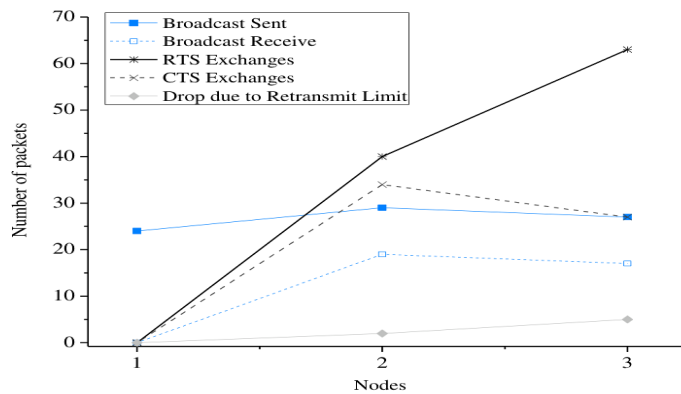


Figure 3. MAC Layer Performance at 40ms^{-1} using AODV protocol

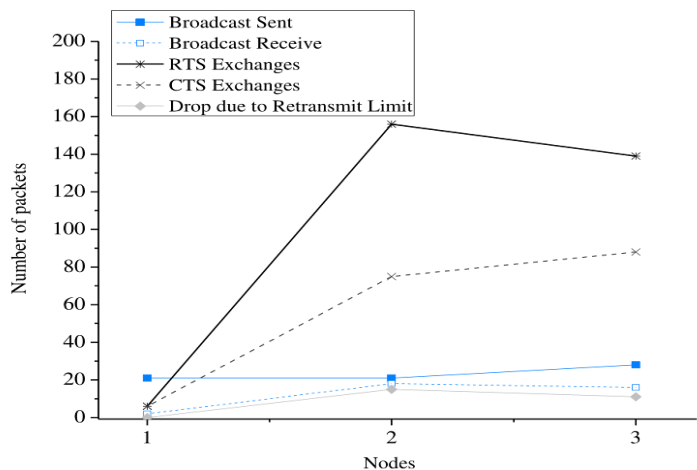


Figure 4. MAC Layer Performance at 40 ms^{-1} using DSR protocol

It is observed that at variable packet rate packet drop is double when DSR is used. Exchanges of broadcast sent and receive is same when uses AODV and DSR but exchanges of RTS is three times at node number 2 uses of DSR. In Figure 1, CTS exchange is half in comparison of DSR protocol used.

protocol used.

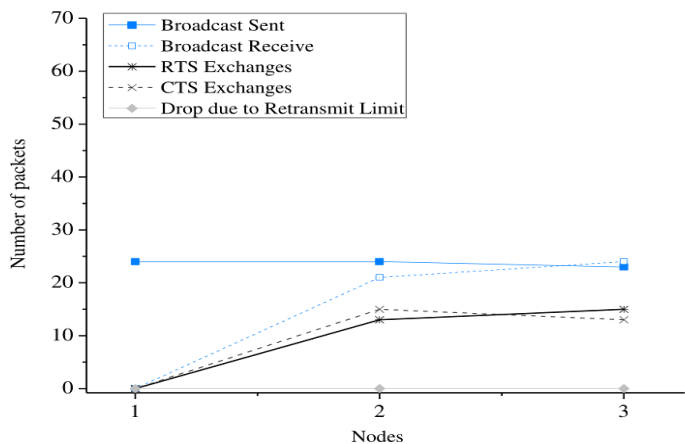


Figure 5. MAC Layer Performance at 10 ms^{-1} using AODV protocol

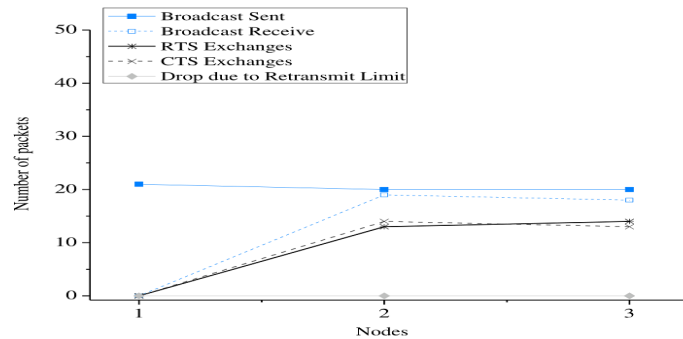


Figure 6. MAC Layer Performance at 10 ms^{-1} using DSR protocol

Figure 5 and Figure 6 shows the MAC performance in terms of broadcast sent, broadcast received, RTS sent, CTS received and drop due to retransmit limit using AODV and DSR respectively at low speed considered 10 ms^{-1} . Packet length is taken variable.

It is observed that at low speed packet drop due to retransmit limit is zero. Packet drop is started when speed of node is 30 ms^{-1} . Below 30 ms^{-1} speed packet drop is zero using AODV and DSR routing protocol. At high speed performance of MAC layer is very poor using DSR protocol. Comparatively Packet drop is very less of MAC protocol using AODV whenever speed of node is high, but zero packet drop due to retransmit limit when speed of node less than 30 ms^{-1} .

Performance of MAC layer is also analyzed at high and low speed while packet rate is constant. Results show that packet drop is high at constant bit rate in every scenario of MAC layer using both AODV and DSR routing protocol. Figure 5-8 are shown the MAC performance at constant bit rate using AODV and DSR speed of node is considered high and low respectively.

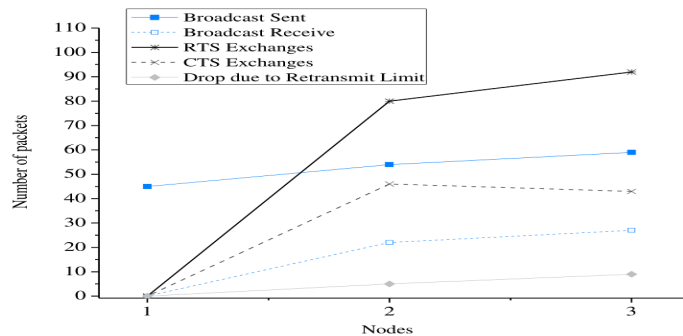


Figure 7. MAC Layer Performance at 40 ms^{-1} using AODV protocol and Constant Bit Rate

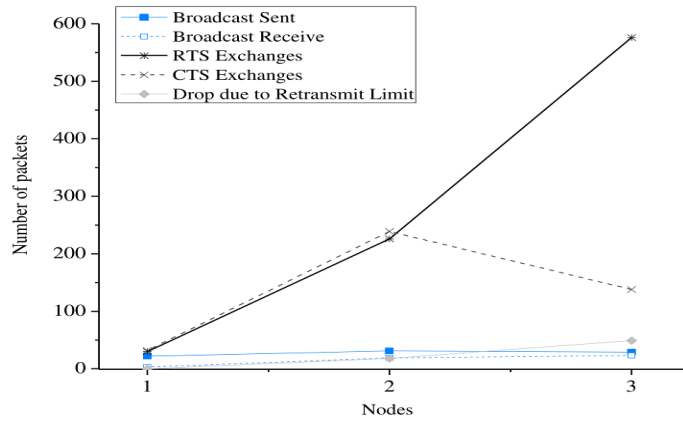


Figure 8. MAC Layer Performance at 40 ms^{-1} using DSR protocol and Constant Bit Rate

Figure 5 and Figure 6 shows the MAC performance in terms of broadcast sent, broadcast received, RTS sent, CTS received and drop due to retransmit limit using AODV and DSR respectively at low speed considered 10 ms^{-1} . Packet length is taken constant. In Figure 6, RTS and CTS exchange is more than around 550 and 130 respectively. Packet drop due to retransmit limit is 18 and 49 of node 2 and node 3 respectively.

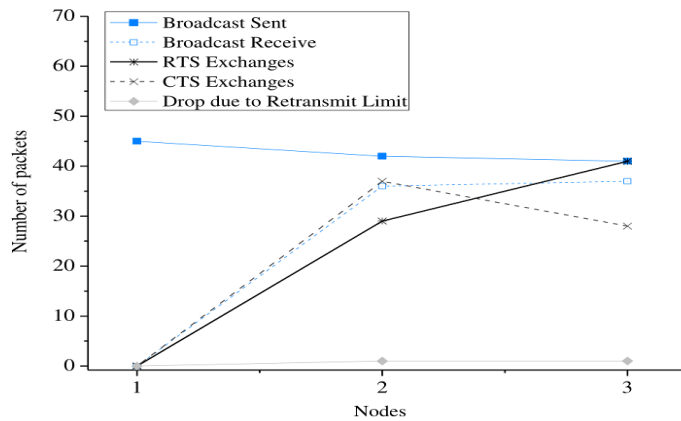


Figure 9. MAC Layer Performance at 10 ms^{-1} using AODV protocol and Constant Bit Rate

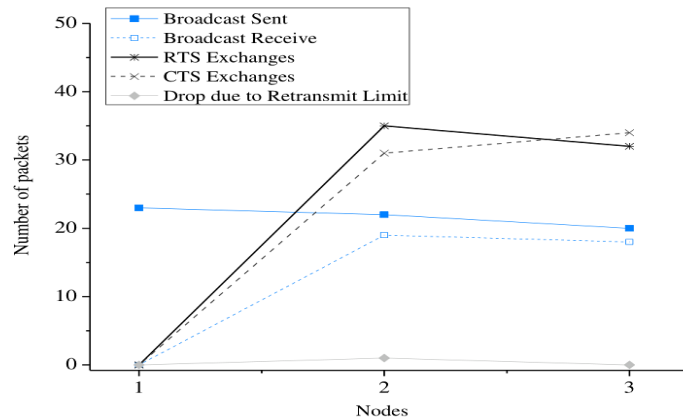


Figure 10. MAC Layer Performance at 10 ms^{-1} using DSR protocol and Constant Bit Rate

In Figure8, packet drop is showing at low speed while at variable bit rate there is no packet drop. The analysis and observation about MAC layer is at high speed packet drop due to retransmit limit is very high using DSR. Packet drop is zero below 30 ms^{-1} speed while packet bit rate is constant. However, packet bit rate is constant then packet drop is very low i.e. 1 at 10 ms^{-1} .

Conclusion

In this paper solution to hidden and exposed terminal problem has been presented on the basis of analysis of MAC layer communication. Also feasibility of MAC layer at high speed has been investigated and proposed to use this for mitigation of exposed terminal at high speed MANETs. The experiment has been done at constant bit rate of packet and variable bit rate to justify the different packet sizes for various networks and nodes. The results of MAC layer were clearly portraying AODV as a better at low speed as compared to DSR. However, packet drop of AODV and DSR is less than at variable bit rate of packet in MANETs. It is also found that hidden and exposed terminal problems can be mitigated having some tradeoffs in the network.

References

- [1] Lu Wang, Kaishum Wu and M. Hamdi, "Combining Hidden and Exposed Terminal Problems in Wireless Networks," IEEE Transactions on Wireless Communications, pp. 1–10, 2012.
- [2] A. Jayasuriya S. Perreau, A. Dadeja and S. Gordon, "Hidden vs. Exposed Terminal Problem in Ad hoc Networks."

-
- [3] R. T. Valadas, A. R. Tavares, A. M. D. Durate, A. C. Moreira and C. T. Lomba, "The Infrared Physical Layer Wireless LAN Standard for Wireless Local Area Networks," IEEE Communications Magazine, Vol. 36, No. 12, pp. 106–112, 1998.
 - [4] IEEE 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.
 - [5] Y.-B. Ko, V. Shankarkumar, and N. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks," IEEE Infocom, Vol. 1, No. 3, pp. 13–21, 2000.
 - [6] E. M. Royer and C-K Toh, "A Review of Current Routing Protocols for ad hoc mobile Wireless Network," IEEE Person. Commun., Vol. 6, No. 2, 1999.
 - [7] Qualnet Simulator, http://systems.cs.colorado.edu/~caleb/qualnet_documentation/QualNet-4.5-ProgrammersGuide.pdf