Performance Analysis of WLAN using OPNET

Tazeem Ahmad Khan, M T Beg, M A Khan

Abstract- Abstract- In this paper analyze the performance of Wireless Local Area Networks (WLANs), it is important to identify what types of network settings can cause bad performance. Low throughput, high packet loss rate, delayed round trip time (RTT) for packets, increased retransmissions, and increased collisions are the main attributes to look for when analyzing poor network performance. We use the OPNET Modeler to simulate the RTS/CTS mechanism to evaluate the performance of IEEE 802.11 MAC protocol. We have simulated two scenarios with and without RTS/CTS mechanism enabled on network nodes. We have concluded our findings by comparing the total WLAN retransmissions, data traffic sent/received, WLAN Delay of two scenarios. RTS/CTS mechanism is helpful to reduce the number of retransmissions if hidden node problem persists in network scenarios.

Key words: RTS/CTS, wireless LAN, MAC layer, opnet.

I. INTRODUCTION

The popular Physical (PHY) layer and Medium Access Control (MAC) sublayer standard for Wireless LAN (WLAN) is provided by IEEE in form of a family of 802.11 protocols. The MAC protocol is the main element that determines the efficiency in sharing the limited communication bandwidth of the wireless channel in WLANs.

The basic access method for 802.11 is the Distributed Coordination Function (DCF), which uses Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA). Since in CSMA/CA, the stations cannot detect the collision there is a possibility of unnecessary bandwidth wastage in case of collision due to completion of transmission by the involved stations. However, the "listen before talk" in CSMA/CA access method used in 802.11 guarantees equal duration of channel access to all devices irrespective of their needs. In other words, when a device with a low bit rate captures the channel, it penalizes other devices using a higher rate by degrading the speed of their connections. For example, when one wireless device connects to a WLAN at a lower bit rate than other devices for being too far from the access point, performance of other network devices degrades.

To combat this problem, a second carrier sense mechanism is available, which enables a station to reserve the medium for a specified period of time through the use of request to send / clear to send (RTS/CTS) frames. In the case described above, far station sends an RTS frame to the AP. The RTS will not be heard by the second station.

The RTS frame contains a duration/ID field which specifies the period of time for which the medium is reserved for a subsequent transmission. Upon receipt of the RTS, the AP responds with a CTS frame, which also contains a duration/ID field specifying the period of time for which the medium is reserved.

Manuscript received on April, 2013.

Tazeem Ahmad Khan, Research Scholar, Department of ECE, F/o Engg & Tech., JMI, New Delhi-25, India.

M T Beg, Prof & Head, E & C Deptt., F/o Engg & Tech., JMI, India.

M A Khan, Prof/HoS, Electrical Engg Section, F/o Engg & Tech., JMI, India.

While the nearer station did not detect the RTS, it will detect the CTS and adjusts accordingly to avoid collision even though some nodes are hidden from other stations.

The hidden node and throughput degradation due to large packets lead to two main solutions. First mechanism allows an RTS Threshold (RT) value that determines when the RTS/CTS handshaking mechanism should be used. So, when the data size is bigger than RT, the optional RTS/CTS mechanism could be used to prevent a loss of channel bandwidth that could otherwise happen due to excessively large data units. The second option that could be used effectively with or without RTS/CTS is the fragmentation. Fragmentation Threshold (FT) is used to limit the size of data packets thus reducing the bandwidth wastage. It is also used to combat the effects of poor channel quality. By reducing the size of the packets transmitted, there is a better probability of successful transmission, especially under poor channel conditions.

The hidden terminals may cause performance degradation in WLANs, which can be controlled by using RTS/CTS mechanism as mentioned above. An optimal WLAN performance may be obtained by adjusting the RTS/CTS threshold while monitoring the impact on throughput. The 802.11 standard requires that a station must refrain from sending a data frame until the station completes a RTS/CTS handshake with an AP

II. WLAN PERFORMANCE ISSUES

The Hidden Terminal Problem

The Hidden terminal or hidden node problem is one of the most common problems in wireless networks. As every station in a wireless network has limited radio transmitting range, it cannot communicate with every other station in the network. A consequence of this is that two stations may try to communicate with the same third station simultaneously which may result in a collision at the third station. This problem can be overcome by incorporating the RTS/CTS mechanism in the network.

RTS/CTS Mechanism

The wireless station ready to transmit is made to send a short Request To Send (RTS) frame before each data frame transmission. A collision of the RTS frame is less probable than the collision of the actual data frame due to a difference is size. If the receiver station is ready to receive, it acknowledges the RTS frame by sending a Clear To Send (CTS) frame to the sender and thus blocks all traffic from other wireless stations. When the source receives the CTS frame, it sends the data frame as the channel has been reserved for the entire length of transmission. Finally, the receiver sends the ACK frame to the sender upon receiving the frame. Hence, using this 4-way handshake mechanism the hidden terminal problem can be resolved.

III. PERFORMANCE EVALUATION

A. Simulation Environment

We have simulated the effectiveness of RTS/CTS mechanism using OPNET [1] Modeler,a network simulator developed by OPNET Technologies Inc. OPNET Modeler incorporates a detailed and accurate model of the physical channel and of the IEEE 802.11 MAC layer. The Two-way ground path loss model is used as radio propagation model. Most of the physical and MAC layer parameters of OPNET are following the IEEE 802.11 standard [6]. A transmission range is about 350 meters due to the transmission power of 15 dBm.

As opnet model, we have placed two nodes and one receiver representing a campus wide WLAN. Receiver, here, will represent an access point for WLAN. We have drawn a trajectory for Node A, on which it will move according to the predefined amount of time and distance. We have set up our simulation such that Node A will move 430 meters (Node A is going out of range of Node B) along the path represented in the Figure 4 over the course of about five minutes.

We have run two scenarios in our simulation to evaluate the effect of RTS/CTS mechanism. Nodes are not using RTS/CTS mechanism in the first scenario while running a simulation. In contrast, Nodes use the RTS/CTS mechanism during the second scenario. Various results are recorded over the course of the 1000 second simulation time.

B. Simulation Results and Discussions

The First Scenario Discussion - Figures 1to 3 show the results belong to the first scenario. Only 800 seconds of simulation results were shown to emphasize the effect of hidden node problem during 350 seconds to 650 seconds

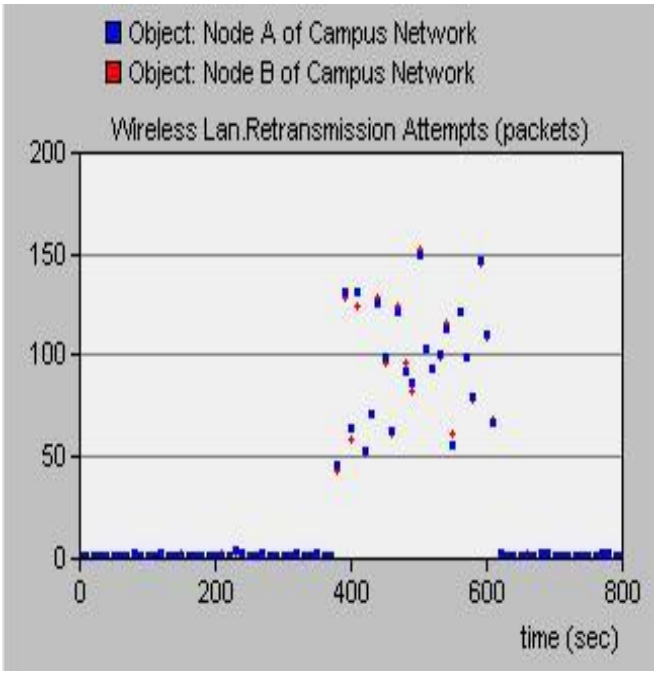

Figure 1 WLAN Data Traffic Sent/Received

Figure 1 shows the WLAN data traffic sent and received in bits/second during simulation time of 1000 seconds. Traffic received statistics indicates WLAN data traffic successfully received by the MAC from the physical layer in bits/sec. Moreover, it includes all data traffic received regardless of the destination of the received frames. While computing the size of the received packets for this statistic, the physical layer and MAC headers of the packet are also included. Traffic Sent statistic represents WLAN data traffic transmitted by the MAC of Node in bits/sec. While computing the size of the transmitted packets for this statistic, the physical layer and MAC headers of the packet are also included.

Due to the defined trajectory pattern, Node A and Node B can no longer see each other, so both nodes no longer receive traffic from one another, as indicated by the data traffic received line in the Figure 1. Since these nodes can't detect each others transmissions, the collision probability for their transmissions increases, which leads to a higher number of collisions and retransmissions [2, 7]. As Node A moved away between 350 and 650 second of simulation, traffic received during the time is almost none.

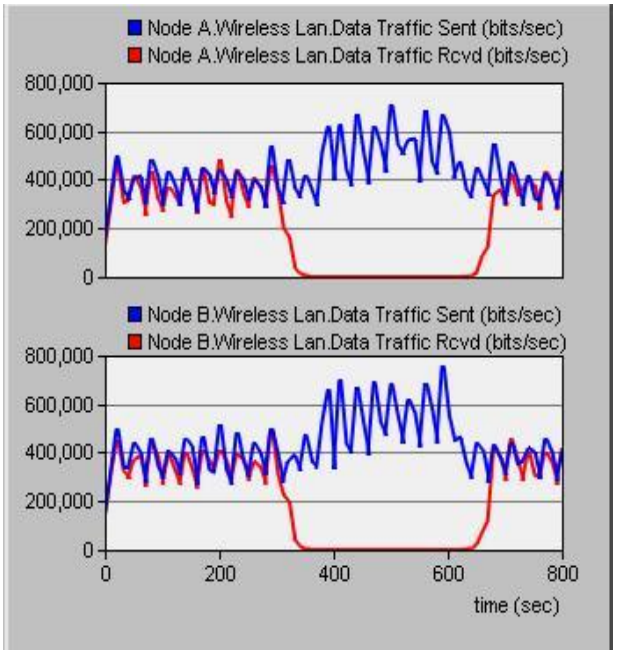

Figure 2 WLAN Retransmission Attempts

Figure 2 shows WLAN retransmission attempts of Node A and Node B. This statistic includes the number of retransmission attempts until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit. You can see that Node A and Node B are having many retransmission attempts during the time when Node A is out of Node B's transmission range. It is due to the collisions of packets sent by both Node A and Node B simultaneously. Numbers of retransmission are between 50 and 100 for both Node A and Node B, while both are hidden from each other.

Once the hidden terminal problem occurs, both nodes increase their retransmission attempts dramatically, which naturally causes more collisions. This increase in collisions slows down the WLAN dramatically as shown in Figure 7. It shows the WLAN Delay which represents the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer.

This delay includes medium access delay at the source MAC, reception of all the fragments individually. It is indicated that WLAN Delay is very high during those retransmissions, while Node A is hidden and out of transmission range of Node B. In short, Figure 1 to 3 shows the same network behavior that show the performance degraded due to hidden terminal problem.

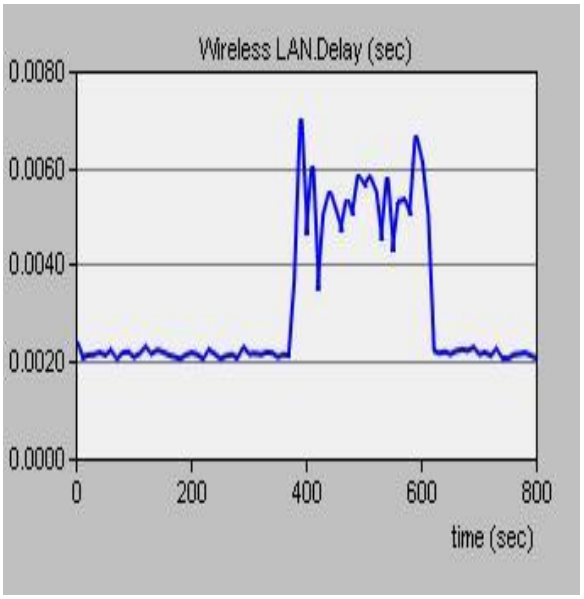

Figure 3 WLAN Delay

The Second Scenario Discussion - Figures 4 to 7 show the results related to the second simulation scenario. In order to reduce the amount of collisions caused by hidden terminal problem, the IEEE 802.11 protocol can use the RTS/CTS mechanism optionally [4, 8]. We have conducted the same experiment, but with the RTS/CTS mechanism enabled on Node A and Node B. This should allow us to eliminate some, but not all of the collisions caused by the hidden terminal problem. Figure 4 shows the comparison of the WLAN data traffic received by Node A for both scenarios. Notice that the traffic received on Nodes A did not change since RTS/CTS is enabled only helpful to prevent collisions from happening.

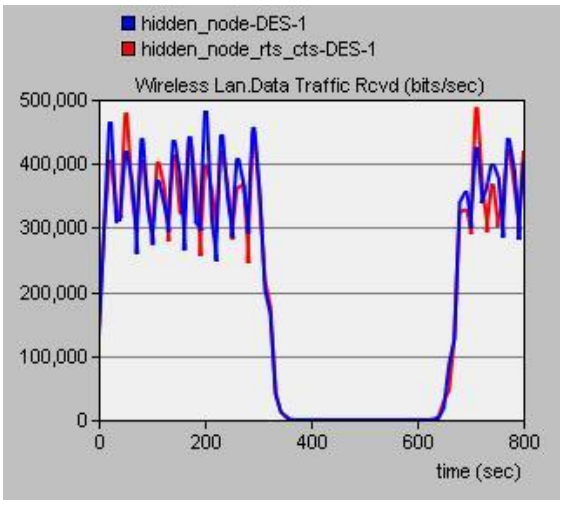

Figure 4 WLAN data traffic Received

Figure 5 shows that WLAN retransmission attempts by Node A. The retransmission attempts did indeed increase a noticeable amount once Node A begins to move. However, the amount of retransmission attempts is up to 8 times fewer than when RTS/CTS was not enabled. This means that there was a significant drop in collisions.

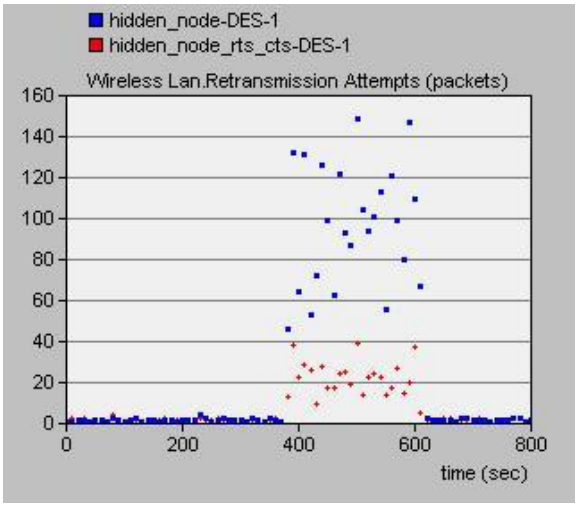

Figure 5 WLAN retransmission attempts

Figure 6 shows WLAN data traffic sent by Node A. The significant drop in collisions had a very large effect on the WLAN sent traffic. Data traffic sent is reduced due to the less number of retransmissions since it is not necessary to keep sending data other nodes within a range are already transmitting (e.g. the Node B and the receiver).

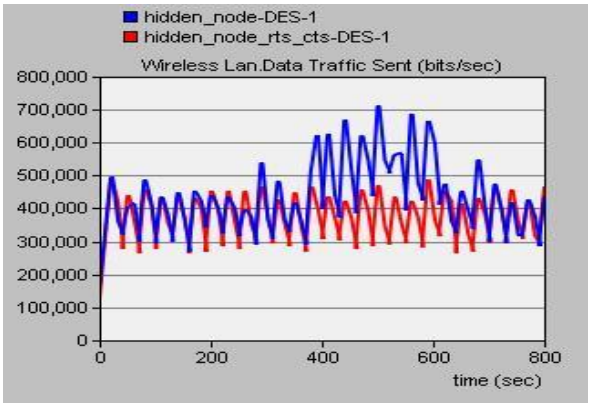

Figure 6 WLAN data traffic Sent

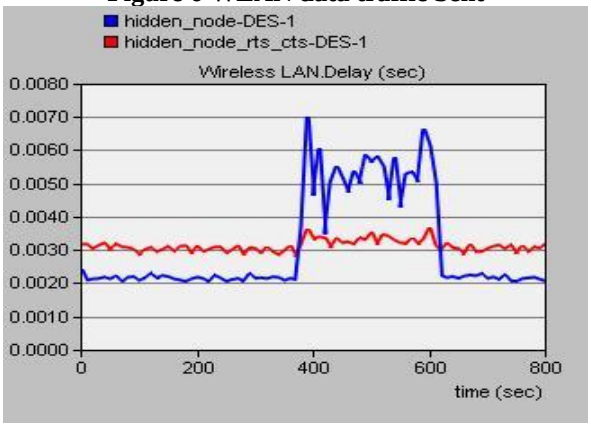

Figure 7 WLAN Delay

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Figure 7 shows the WLAN Delay. Due to less number of retransmissions, the wireless LAN delay drops drastically for the period when the nodes are hidden to each other. It is important to note that the delay is now little higher when

Node A and B can hear each other (when they are not hidden from each other). It is due to the overhead caused by the RTS/CTS handshake mechanism.

C Analysis

From these results, it appears that the RTS/CTS handshake mechanism helps to improve the WLAN performance when nodes are hidden from each other. The WLAN outgoing traffic stayed at a constant rate, even though Node A was in motion and moving away (hidden from Node B).

According to the results of our simulations, motion doesn't have a big impact as we originally suspected. There were some increases in collisions in terms of actual collected data, but chances are that an end user would not notice them. This simulation also shows that proper configuration of all network devices is extremely important. With RTS/CTS disabled, network performance dropped significantly and in fact it may have rendered many services unusable. With RTS/CTS enabled, LAN delay stayed around 30ms, out going traffic remained stable, and collisions were kept to a minimum.

At 350 seconds, Node A becomes a hidden node to Node B (and vice versa) for approximately 300 seconds. During this period, use of RTS/CTS frame exchange reduces the number of collisions (and therefore retransmissions) significantly. CTS message sent by the Receiver node informs the sender nodes about the upcoming data transmission attempt of the other node and its reservation of the channel.

IV. CONCLUSIONS

It is important to evaluate the effectiveness of optional RTS/CTS handshake mechanism on the performance to analyze the IEEE 802.11 based Wireless Local Area Networks (WLANs). When analyzing the performance of IEEE 802.11 based wireless network, throughput, packet loss rate, round trip time (RTT) for packets, number of retransmissions, and number of collisions are the parameters to look for. We use the OPNET Modeler to simulate the RTS/CTS mechanism to evaluate the performance of IEEE 802.11 MAC protocol. We have simulated two scenarios with and without RTS/CTS mechanism enabled on network nodes. We have analyzed our findings by comparing the total WLAN retransmissions, data traffic sent/received, WLAN Delay of mentioned scenarios. In hidden node problem situation, it is useful to enable the RTS/CTS mechanism for mobile nodes. However, it is vital to remember that it also increases the overhead of RTS and CTS packets. For scenarios where hidden terminal problem may not exist, it is better to avoid using an optional RTS/CTS handshake mechanism for IEEE 802.11 based wireless networks.

FUTURE SCOPE

We have tested the affects of mobility on the performance of the IEEE 802.11 based network. Future simulations will involve terrain change, elevation change, and multiple floored buildings. We plan on having multiple scenarios for each situation. When testing mobility, for example, we will simulate nodes moving slower than in the scenario mentioned above, and then nodes dramatically faster, such as a car driving by. Transceiver pipeline modeling is also a part of OPNET that will allow us to model many customizable aspects of wireless simulation. It will allow us to calculate all the propagation delays, different antenna gains, and noise to interference ratios. We will also be able to replicate not only terrain but foliage, weather conditions, and any other natural event that could cause signal degradation [3, 10]. This pipeline lets us model every aspect stacked on top of each other. This will allow an accurate representation of a real wireless network.

In future simulations we will also use different types of network topologies. The simulation that we had run was only an Ad Hoc network [9] and we would like to use an infrastructure network. This will allow us to see and compare data between the infrastructure and Ad Hoc modes of wireless networking. With all these tools we will be able to replicate actual environments to do our testing of the wireless networks for different mobility scenarios.

REFERENCES

1. Online Documentation, "OPNET Modeler," http://www.opnet.com/, Date visited: March 2007.
2. A. Tsertou and D. I. Laurenson, "Insights into the hidden node problem," Proceeding of the 2006 international conference on Communications and mobile computing, pp. 767-772, 2006.
3. K. Xu, M. Gerla, and S. Bae, "How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks?" IEEE GLOBECOM'02, Vol. 1, pp. 72-76, November 2002.
4. A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and techniques for diagnosing faults in IEEE802.11 infrastructure networks," Proceedings of the 10th annual international conference on Mobile computing and networking, pp. 30-44, 2004.
5. Michael Zhonghua Jiang, "Analysis of Wireless Data Network Traffic,"University of Science and Technology of China, M.A.Sc. Thesis, April 2000.
6. IEEE, "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specification," IEEE 802.11 Draft Version 4.0, May 1996.
7. K. Xu, M. Gerla, and S. Bae, "Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks," Ad Hoc Networks, Elsevier, vol. 1, no. 1, pp. 107-123, 2003.
8. S.Ray, J.B.Carruthers, and D.Starobinski, "RTS/CTS-induced congestion in ad hoc wireless LANs," In WCNC, 2003.
9. C. K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, December 2001.