DOI: 10.15415/jtmge.2010.11007

Journal of Technology Management for Growing Economies

Volume 1 Number 1 **April 2010**

Analysis of Exposed Node Problem and Security Concerns in Adhoc Networks

T. L. Singal
Chitkara Institute of Engineering and Technology, Rajpura, Punjab
Prachi Sharma
Ravneet Kaur
Infosys Technologies Ltd., Mysore

CHITKARA UNIVERSITY

Analysis of Exposed Node Problem and Security Concerns in Adhoc Networks

T. L. Singal
Chitkara Institute of Engineering and Technology, Rajpura, Punjab
Prachi Sharma
Ravneet Kaur
Infosys Technologies Ltd., Mysore

Abstract

The paper contains the analysis of exposed node problem in mobile adhoc network. The problem is that before starting the transmission, a station wants to know whether there is activity around the receiver. If the transmission is taking place around the receiver, there will be collisions and the effective throughput will be decreased. A detailed study of the simulation on these exposed nodes is carried out using the GloMoSim software to calculate the throughput for the various transmission powers and different protocols, so as to compare the performances by varying different parameters. These simulation results with GloMoSim corroborate our theoretical analysis.

Keywords: Exposed node, Adhoc network, Simulator, MANET, GloMoSim, AODV, CSMA.

INTRODUCTION

For this paper, we have used GloMoSim 2.0, a network simulator with strong origins in scalable, mobile, wireless research and an evolving wired component, as our simulation tool. For large-scale networks with thousands of nodes, timely execution of a simulation is desirable, and increased abstraction of network models can be exercised to speed up simulation.

A mobile ad hoc network (MANET) is a wireless network temporarily and spontaneously created by mobile stations without requiring any infrastructure or central control. Network management tasks and communications are typically performed in a distributed manner. An ad-hoc wireless network is a network without any base stations, an 'infrastructure less' network. In such a network each mobile host acts as a router, peer-to-peer communications are possible as well as peer-to remote communications. These features make MANETs very practical and easy to deploy in places where existing infrastructure is not capable enough to allow communication, e.g. in disaster zones, or infeasible to deploy. At the same time it creates huge problems as well. One problem lays in design of the Medium Access Control (MAC) Protocols which define how the wireless medium is shared by all nodes. It is possible to design a MAC protocol that can handle the sharing of the medium but at the same time has proved to be one of the most challenging tasks for the researchers. Due to the nature

Journal of Technology Management for Growing Economies
Vol. 1 No. 1, April 2010
pp.103-112

of the network distributed random access MAC is preferred over centralized MAC; however distributed random access protocols suffer from Hidden and Exposed nodes issues. (Talukdar and Yawagal, 2005; Gummalla and Limb, 2000).

BACKGROUND

Carrier Sense Multiple Access (CSMA) is one of the earliest mechanisms adopted for ad hoc networks. In CSMA, a transmitter will first sense the wireless channel in the vicinity and refrain itself from transmission if the channel is already in use. Various methods such as ALOHA and n-persistent algorithms can be used to determine how long the deferred node should wait before the next attempt. CSMA introduces hidden node and exposed node problems. It is assumed that each node can communicate with another node only if there is a link between them. In a typical exposed node problem a node within the range of the transmitter may be unnecessarily prohibited from accessing the medium and thus decreases the network throughput (Xu et al, 2002).

EXPOSED NODE PROBLEM

In wireless networks, the exposed node problem occurs when a node is prevented from sending packets to other nodes due to a neighboring transmitter (ANSI/IEEE Standards 802.11, 1999; Xu et al., 2003). Consider an example of 4 nodes labeled A, B, C, and D, where the two receivers are out of range of each other, yet the two transmitters in the middle are in range of each other. Here, if a transmission between A and B is taking place, node C is prevented from transmitting to D as it concludes after carrier sense that it will interfere with the transmission by its neighbor A. However note that D could still receive the transmission of C without interference because it is out of range from A.

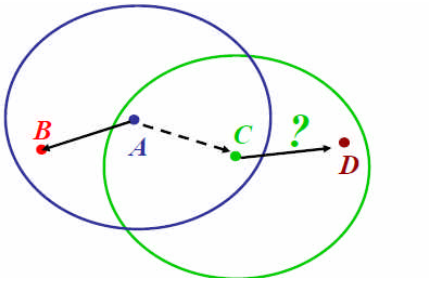

Figure 1: Exposed Node Problem

In the exposed node problem we use the free space propagation model. The free space propagation model is used to predict received signal strength when the transmitter and receiver have a clear, unobstructed line-of-sight between them. This model predicts that transmission power is attenuated in proportion to the square of the distance. According to this model, the *Friis Free Space Equation* for non-isotropic antennas is the following:

$$P_r = P_t(?/4pd)^n G_t G_r \quad (1)$$

where P_r is the received power, P_t is the transmitted power (in watts or milliwatts), is the carrier wavelength (in meters), d is the distance between transmitter and receiver (in meters), n is the path loss coefficient, G_t is the antenna gain at the transmitter and G_r is the antenna gain at the receiver (dimensionless).

For the *Ideal Isotropic Antenna*, the free space loss equation is:

$$P_t/P_r = (4p\,d)^2/?^2 = (4p\,fd)^2/c^2 \quad (2)$$

where c is the speed of light (3 x 10^8 m/s) and f is the frequency (in hertz or 1/s).

SIMULATION USING GLOMOSIM

A comparative study of five nodes in case of Free Space condition using the AODV routing algorithm with CSMA protocol and Bellmanford routing algorithm with IEEE 802.11 protocol led to the results which are tabulated in Table 1 and 2. (URL:http://www.isi.edu/nsam/ns) (URL:http://pcl.cs.ucla.edu/projects/glomosim).

a) Transmission power : +7 dBm
   Receiver threshold power: -91 dBm
   Inter nodal distance: 750 m

Table 1: Throughputs at Transmission power +7dBm, Receiver threshold power -91dBm with CSMA protocol.

TRANSMISSION	THROUGHPUT (IN BPS)	
	AODV (CSMA)	BELLMANFORD (CSMA)
Node 0-1	551115	646779
Node 0-2	1047	5712.5
Node 1-0	10536	738709.5
Node 1-2	357473	1268.5
Node 2-0	536894.5	543858.5
Node 2-1	12068.5	36933

Table 2: Throughputs at Transmission power +7dBm, Receiver threshold power -91dBm with 802.11 protocol.

TRANSMISSION	THROUGHPUT (IN BPS)	
	AODV (802.11)	BELLMANFORD (802.11)
Node 0-1	841464.5	831170
Node 0-2	52364.5	18302
Node 1-0	330746.5	317766.5
Node 1-2	147347.5	92400.5
Node 2-0	238780	33345
Node 2-1	136761	52392

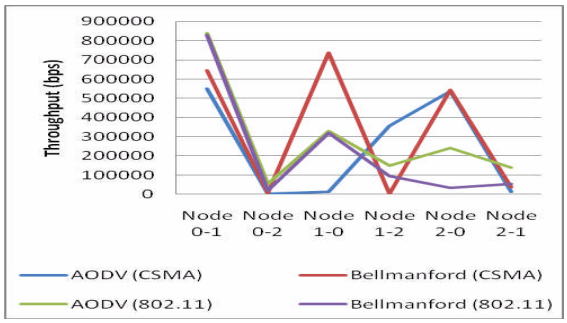

Figure 2: Comparative graph of throughputs at Transmission power +7dBm and receiver threshold power -91dBm

a) Transmission power : +7dBm
Receiver threshold power: -81dBm
Inter nodal distance: 200m

Table 3: Throughputs at Transmission power +7 dBm, Receiver threshold power -81dBm with CSMA protocol.

TRANSMISSION	THROUGHPUT (IN BPS)	
	AODV (CSMA)	BELLMANFORD (CSMA)
Node 0-1	809225	656469
Node 0-2	19221	115007.5
Node 1-0	135746	61930
Node 1-2	272906.5	216460
Node 2-0	304651	520243.5
Node 2-1	9930	136088

Table 4: Throughputs at Transmission power +7dBm, Receiver threshold power -81dBm with 802.11 protocol.

TRANSMISSION	THROUGHPUT (IN BPS)	
	AODV (802.11)	BELLMANFORD (802.11)
Node 0-1	776551.5	793729.5
Node 0-2	137876	26597.5
Node 1-0	232701.5	291210
Node 1-2	53939.5	37003
Node 2-0	243453	32411.5
Node 2-1	257715.5	93691.5

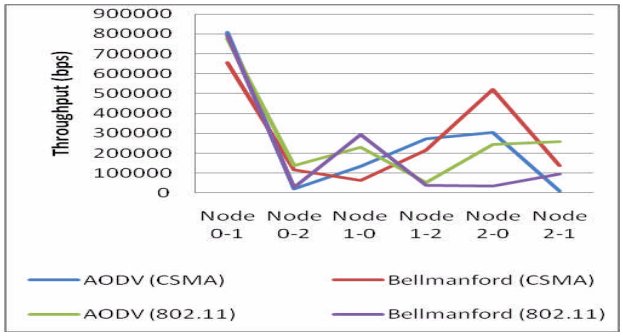

Figure 3: Comparative graph of throughputs at Transmission power +7dBm and receiver threshold power -81dBm.

b) Transmission power : +15dBm
Receiver threshold power: -81dBm
Inter nodal distance: 620m

Table 5: Throughputs at Transmission power +15dBm, Receiver threshold power -81dBm with AODV protocol.

TRANSMISSION	THROUGHPUT (IN BPS)	
	AODV (CSMA)	BELLMANFORD (CSMA)
Node 0-1	668945.5	583711.5
Node 0-2	6321.5	4811.5
Node 1-0	206841.5	585853
Node 1-2	272453	332701.5
Node 2-0	1096	519583
Node 2-1	36753	37015.5

Table 6: Throughputs at Transmission power +15dBm, Receiver threshold power -81dBm with AODV protocol.

TRANSMISSION	THROUGHPUT (IN BPS)	
	AODV (802.11)	BELLMANFORD (802.11)
Node 0-1	781547.5	590757
Node 0-2	137820.5	24754
Node 1-0	250923.5	296680.5
Node 1-2	53854.5	36929.5
Node 2-0	242910	33211
Node 2-1	257707	89446.5

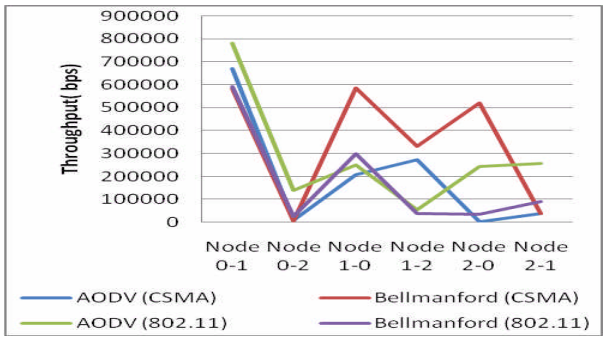

Figure 4: Comparative graph of throughputs at Transmission power +15dBm and receiver threshold power -81dBm.

c) Transmission power : +15dBm
Receiver threshold power: -91dBm
Inter nodal distance: 1950m

Table 7: Throughputs at Transmission power +15dBm, Receiver threshold power -91dBm with AODV protocol.

TRANSMISSION	THROUGHPUT (IN BPS)	
	AODV (CSMA)	BELLMANFORD (CSMA)
Node 0-1	362965.5	413134.5
Node 0-2	517	2664
Node 1-0	30177.5	738375
Node 1-2	357473	1268.5
Node 2-0	537063	548758.5
Node 2-1	34503.5	36925

Table 8: Throughputs at Transmission power +15dBm, Receiver threshold power -91dBm with AODV protocol.

TRANSMISSION	THROUGHPUT (IN BPS)	
	AODV (802.11)	BELLMANFORD (802.11)
Node 0-1	841467	818236
Node 0-2	52125	25036.5
Node 1-0	324824.5	334953.5
Node 1-2	146431	91925
Node 2-0	237455.5	20089
Node 2-1	136749	16877

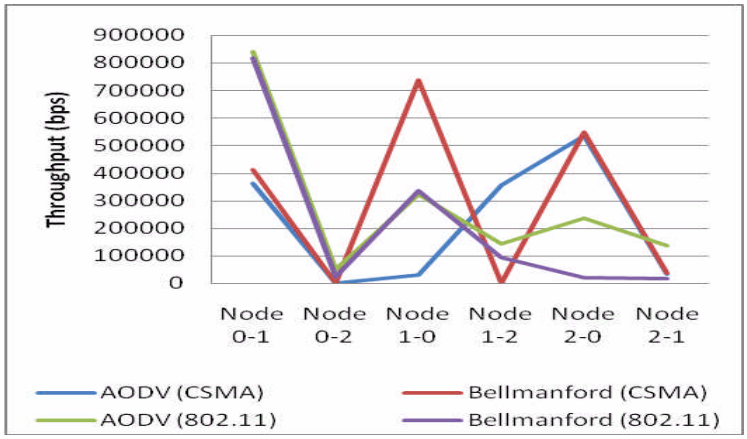

Figure 5: Comparative graph of throughputs at Transmission power +15dBm and receiver threshold power -91dBm.

MITIGATING THE EXPOSED NODE PROBLEM

IEEE 802.11 RTS/CTS mechanism helps to solve this problem only if the nodes are synchronized. When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an exposed node and is permitted to transmit to other neighboring nodes. If the nodes are not synchronized the problem may occur that the sender will not hear the CTS or the ACK during the transmission of data of the second sender. (Saeed et al, 2007).

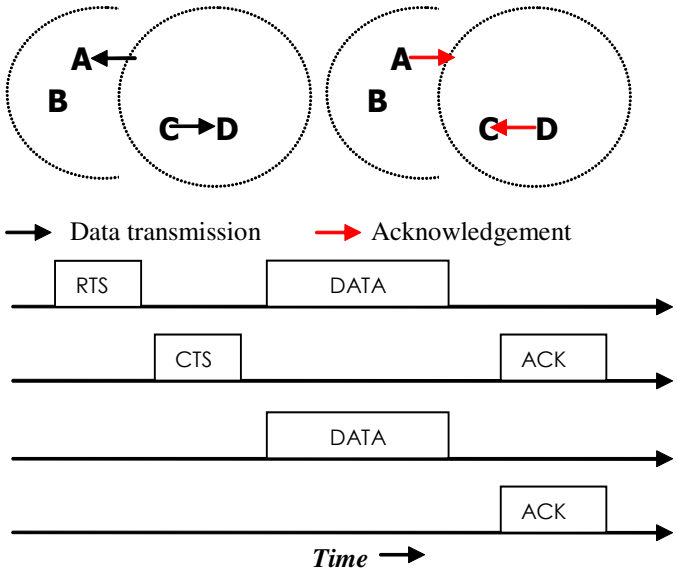

Figure 6: Mitigating Exposed Node Problem

RESULTS AND ANALYSIS

The following results are drawn from the above analysis: No throughput is observed on node 3 & 4 because of the exposed node problem. On increasing the transmitter power, at the threshold distances respectively, the throughputs at individual nodes also increases. The throughput also increases with the increase in receiver threshold power at the threshold distances respectively. The AODV algorithm shows greater throughputs on nodes with 802.11 protocol. The Bellman ford algorithm shows higher throughputs with CSMA protocol than AODV algorithm.

SECURITY IN ADHOC NETWORKS

Ad hoc networks do not have a centralized piece of machinery such as a name server, which if present, as a single node can be a single point of failure. The absence of infrastructure and the subsequent absence of authorization facilities impede the usual practice of establishing a line of defense, distinguishing nodes as trusted and no trusted. Freely roaming nodes form transient associations with their neighbors, joining and leaving sub domains independently with and without notice. An additional problem related to the compromised nodes is the potential Byzantine failures encountered within mobile ad hoc network (MANET) routing protocols wherein a set of nodes could be compromised in such a way that incorrect and malicious behavior cannot be directly noted at all. Such malicious

nodes can also create new routing messages and advertise nonexistent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failures on the system. The wireless links between nodes are highly susceptible to link attacks, which include passive eavesdropping, active interfering, leakage of secret information, data tampering, impersonation, message replay, message distortion, and denial of service (DoS). The presence of even a small number of adversarial nodes could result in repeatedly compromised routes; as a result, the network nodes would have to rely on cycles of timeout and new route discoveries to communicate. This would incur arbitrary delays before the establishment of a non-corrupted path, while successive broadcasts of route requests would impose excessive transmission overhead. In particular, intentionally falsified routing messages would result in DoS experienced by the end nodes. Moreover, the battery-powered operation of ad hoc networks gives attackers ample opportunity to launch a DoS attack by creating additional transmissions or expensive computations to be carried out by a node in an attempt to exhaust its batteries. Attacks against MANET's can be divided into two groups:

Passive attacks typically involve only eavesdropping of data whereas active attacks involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data.

External attacks are typically active attacks that are targeted to prevent services from working properly or shut them down completely (Bhargava and Agrawal, 2001)

Intrusion prevention measures like encryption and authentication can only prevent external nodes from disrupting traffic, but can do little when compromised nodes internal to the network begin to disrupt traffic. Intrusion detection systems provide audit and monitoring capabilities that offer the local security to a node and support the other nodes (Zhang and Lee, 2000). Intrusion detection can be defined as the automated detection and subsequent generation of an alarm to alert the security apparatus at a location if intrusions have taken place or are taking place. As the name implies, these systems detect intrusion attempts and prevents intrusion attempts and prevents intrusion by killing the connection. These IDS systems are installed at the choke point to monitor the complete traffic. These systems operate traffic. These systems operate to promiscuous mode, i.e., the IDS cannot be accessed by any other system. They have a database of thousands of events signatures corresponding to various intrusions attempts. When the IDS system identifies a connection resembling an intrusion event, the connection is killed. Normally,

- The IDS are put at network level after the router for protecting the likely intrusions from outside.
- But they are also kept in important segments of the intranet.

- In addition, host level IDS are also installed on important servers to protect them from intrusions

CONCLUSION

The exposed node problem in wireless adhoc networks has been analyzed with five wireless nodes by taking simulated data. The network scenario has been analyzed using Network Simulator GloMoSim under free-space environment conditions using AODV routing algorithms with CSMA protocol. The results are tabulated and presented in graphs to depict comparison for throughputs at defined Tx power and receiver threshold power has been shown. A comparative study of throughput under different operating conditions and system parameters show that exposed node problem is significantly minimized using IEEE 802.11 RTS/CTS mechanism. The stringest requirement of security aspects in wireless adhoc networks impose compromise in rerouting data to use non-corrupted paths and successive broadcasts of route requests. The results can be further extended for mobile environment and more number of wireless nodes with mobility.

REFERENCES

ANSI/IEEE Standards 802.11, (1999) '*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*'.

Bhargava, S. and Agrawal, D.P. (2001) '*Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks'*, Vehicular Technology Conference, 7-11 Oct., Atlantic City, NJ.

Gummalla, C.V. and Limb, J.O. (2000) '*Wireless medium access control protocols*,' IEEE Communications Surveys & Tutorials, 3, 2-15.

Saeed, M. J., Merabti, M. and Skwith, R.J. (2007) '*Route Maintenance in Wireless Ad Hoc Networks*', paper presented at PGNet2007, 28-29 June, Liverpool John Moores University.

Talukdar, A.K. and Yawagal, R. (2005) '*Mobile Computing*', (1st Ed), Tata Macgraw Hill, pp 324-326.

URL:http://pcl.cs.ucla.edu/projects/glomosim

URL:http://www.isi.edu/nsam/ns

Xu, K., Gerla, M. and Bae, S. (2002) '*How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks?'*, IEEE Globecom'02, 17-21 November, California University, Los Angeles, USA.

Xu, K., Gerla, M. and Bae, S. (2003) '*Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks'*, 1, 107-123.

Zhang, Y. and Lee, W. (2000) '*Intrusion Detection in Wireless Ad Hoc Networks*,' 6th International Conference on Mobile Computing and Network, 6-11 August, pp. 275–283.

T.L. Singal is Professor in ECE Department, Chitkara Institute of Engineering and Technology, Rajpura, Punjab.

Prachi Sharma is System Engineer in Infosys Technologies Ltd., Mysore, India.

Ravneet Kaur is System Engineer in Infosys Technologies Ltd., Mysore, India.

Chitkara University
Saraswati Kendra, Plot 11-12, Dainik Bhaskar Building
Sector 25-D, Chandigarh-160014, India
Email: journal@chitkarauniversity.edu.in
Website: www.chitkara.edu.in/journal/index.php