Anonymous Ad Hoc Network Performance Degradation Analysis in the Presence of Selfish

R.Kalpana
Associate Professor, Computer Science and Engineering
Vivekanandha Institute of Engineering and Technology for women
Tiruchengodu, India.

Dr.N.Rengarajan
Principal, K.S.R. College of Engineering
Tiruchengogu, India.

***Abstract*—Wireless Ad Hoc networks are characterized by dynamic change in topology, infrastructure-less architecture and creation of a network on the fly. Being wireless and co-operative in nature Ad Hoc networks are more prone to security breaches compared to their wired counterparts in all layers of the network. Most security protocols do not address the anonymity issues which can be gathered by a passive eavesdropper who can gather node identity, node location and other network information. Another issue that will affect an Ad hoc network is the non co-operation of nodes which could be selfish or malicious. In this paper we investigate the performance degradation of a dynamic anonymous ad hoc network with various degrees of selfishness. The results obtained are compared with all nodes co- operating and with all selfish nodes eliminated in the network.**

Keywords-Ad hoc Network, Selfish nodes, Malicious nodes, Anonymous network.

I. INTRODUCTION

Wireless networks can be broadly classified into infrastructure based networks and infrastructure-less networks. Infrastructure based network uses access point for communication between the wireless nodes and to the wired external network. All wireless nodes in the network are identified by the same SSID. In the case of infrastructure-less network or ad hoc networks there is no pre existing infrastructure or centralized control. Ad hoc networks are growing in popularity and are believed to drive the next 4G networks. Ad hoc networks find applications in the areas of disaster management, military and business[1]. Traditional routing protocols used in wired networks are ineffective for ad hoc networks due to the inherent qualities of wireless media and the changing topology of the network. Various routing protocols have been proposed for Ad hoc networks and can be broadly classified into table drive routing protocols and on demand routing protocols. Table drive routing protocols create routing table irrespective of communication between nodes. This can be of disadvantage in high mobility and large networks. Routing protocols falling under this scheme are the Distance sequenced distance vector (DSDV) routing protocol[2] an extension of Distance vector routing protocols and Optimized link state routing protocol (OLSR) [3]. On demand routing protocols on the other hand create the routes between the source and destination node only when the source wants to communicate with the destination node. Popular routing protocols in this category are the Dynamic source routing (DSR)[4] and Ad hoc on demand distance vector (AODV) routing protocol[5]. Most of the routing protocols initially proposed do not offer any sort of security features.

Security was not considered in the initial drafts of Ad hoc routing protocols. Attacks in a Ad hoc network can either be active attacks or passive attacks. Key security features that are expected in an Ad hoc network are authentication, confidentiality, availability, anonymity, integrity and non repudiation. Active attacks interrupt or degrade the quality of service in the network by various methods including denial of service, worm hole attack, spoofing, replay attacks and altering the control overhead packets by changing its information. Passive attacks on the other hand silently listen or extract vital information in the data packets. Active attacks are easier to detect compared to passive attacks due to the degradation of QOS. Popular routing protocols to overcome attacks include Adaptive routing for Ad hoc network (ARAN)[6] routing protocol which uses asymmetric cryptographic techniques, Secure aware Ad hoc routing (SAR)[7] which uses security metrics in the Route request (RREQ) messages and nodes should have the decryption keys to decrypt the data for receiving and forwarding. Another proposed secure routing protocol based on symmetric cryptography is the secure routing protocol (SRP) [8] where a security association (SA) is required between the source and destination nodes. Keys generated by the SA are used to encrypt and decrypt the data.

Though anonymity is part of security most routing protocols addressing the security issues by authentication and cryptographic means have not addressed the anonymity of communication between nodes. Anonymous

communication ensures source and destination anonymity so that adversaries will find it difficult to distinguish sources and destinations from forwarders and communication relations anonymity which ensures the adversary cannot identify linkability. Popular anonymous routing protocols include Anonymous on demand routing (ANODR) protocol[9], Anonymous routing protocol for mobile ad hoc network(ARM), Secure distributed anonymous routing protocol (SDAR)[10] and Anonymous dynamic source routing (AnonDSR)[11].

In an Ad hoc network nodes are classified into failed nodes, co operative nodes, selfish nodes and malicious nodes. A node can fail to be in the active part of the network as it moves out of transmission range or being switched off due to a malfunction. Failed nodes are not used during the route discovery process. Co-operative nodes are active in the network and participates in the route discovery and packet forwarding. Selfish nodes are actively involved in route discovery and would actively involve sending and receiving its own packets, however they tend to drop data packets of other nodes either fully or selectively to reduce their cpu processing and save battery. These nodes drastically affect the performance of the network. On the other hand malicious nodes are active in route discovery and may involve in the transfer of data packets similar to selfish nodes or a co-operative node. However they are involved in launching attacks on the network either to disrupt the service or steal data from the network.

Though performance evaluation of various routing protocols under different mobility and size scenarios have been studied extensively, the effect of selfish nodes in an anonymous network has not been studied to a large extent. In this paper we study the performance of an Ad hoc network with nodes behaving with various degrees of selfishness. This study finds importance as the implementation of ad hoc networks become popular, and the co operation of nodes will be of utmost importance for the efficient operation of the network. In the next section we describe the experimental setup along with the results obtained and in the last section we discuss the results obtained and conclude this paper.

II. EXPERIMENTAL SETUP

The simulation environment consists of 20 nodes. Each node runs a client-server application over TCP/IP. The data rate of each node is 11 Mbps with a transmit power of 0.005 watts. The nodes are distributed for 4 sq Km.The trajectory of the nodes are random and follow no fixed path. One of the node is assigned as a mobile server. The initial layout is shown in figure I. Experiments were conducted to simulate the following scenarios.

FTP load with all nodes co operating

FTP load with 15% of nodes being selfish

FTP load with all selfish nodes failed.

Database query load with all nodes co operating

Database query load with 15% of nodes being selfish

Database query load with all selfish nodes failed.

As seen from figure I, some of the nodes can reach the server node in one hop whereas other nodes may take more than two hops to reach the server. Node 1, node 3 and node 7 are designed as selfish nodes. Selfish node 1 is designed to drop packets that has to be sent to node 0, node 2 and node 9. Selfish node 3 is designed to drop packets that has to be sent to node 13 and node 7 drops all node to be sent to node 12. The throughput obtained for the FTP load and Database query load is indicated in figure II and figure III.

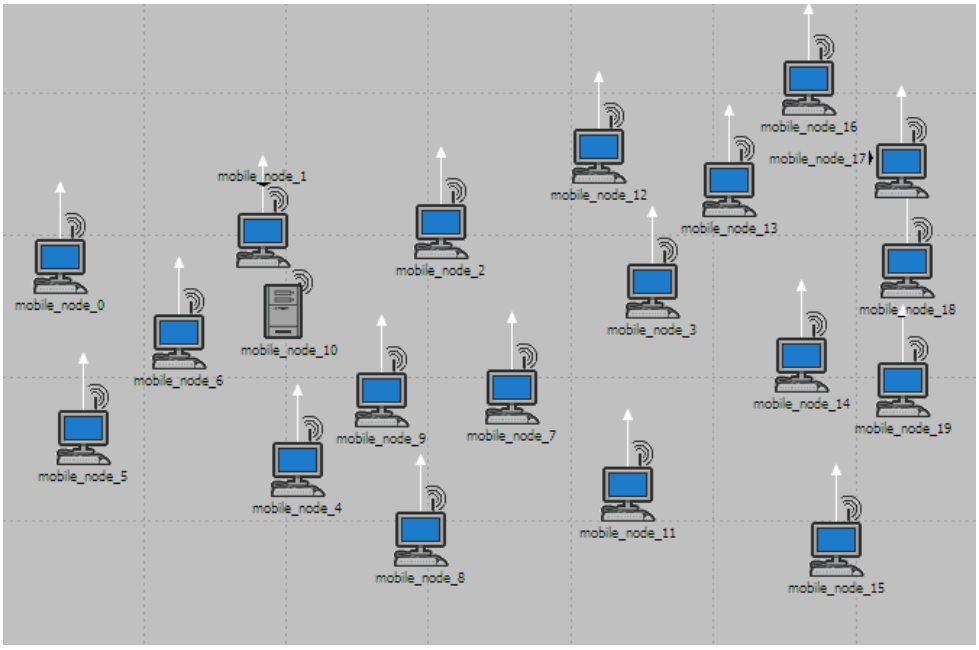

Figure I : The layout used in our simulated environment.

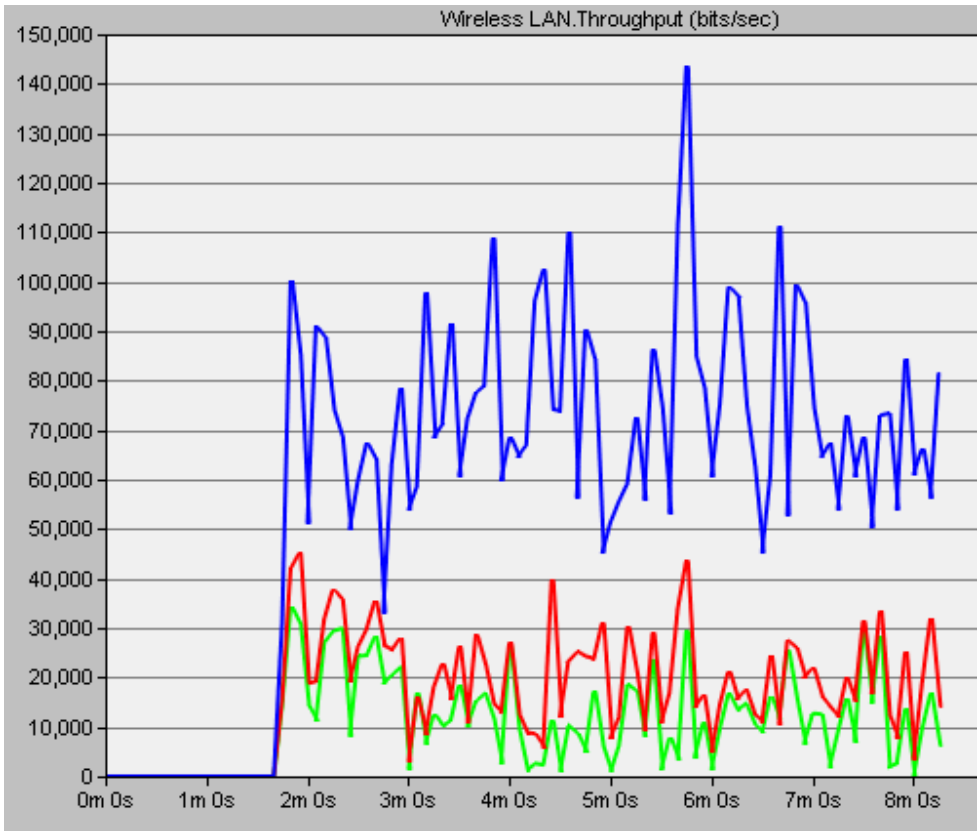

Figure II. Throughput obtained for database load with fully co operative nodes (blue), 15% selfish nodes participating in network(red) and selfish nodes not participating in the network.

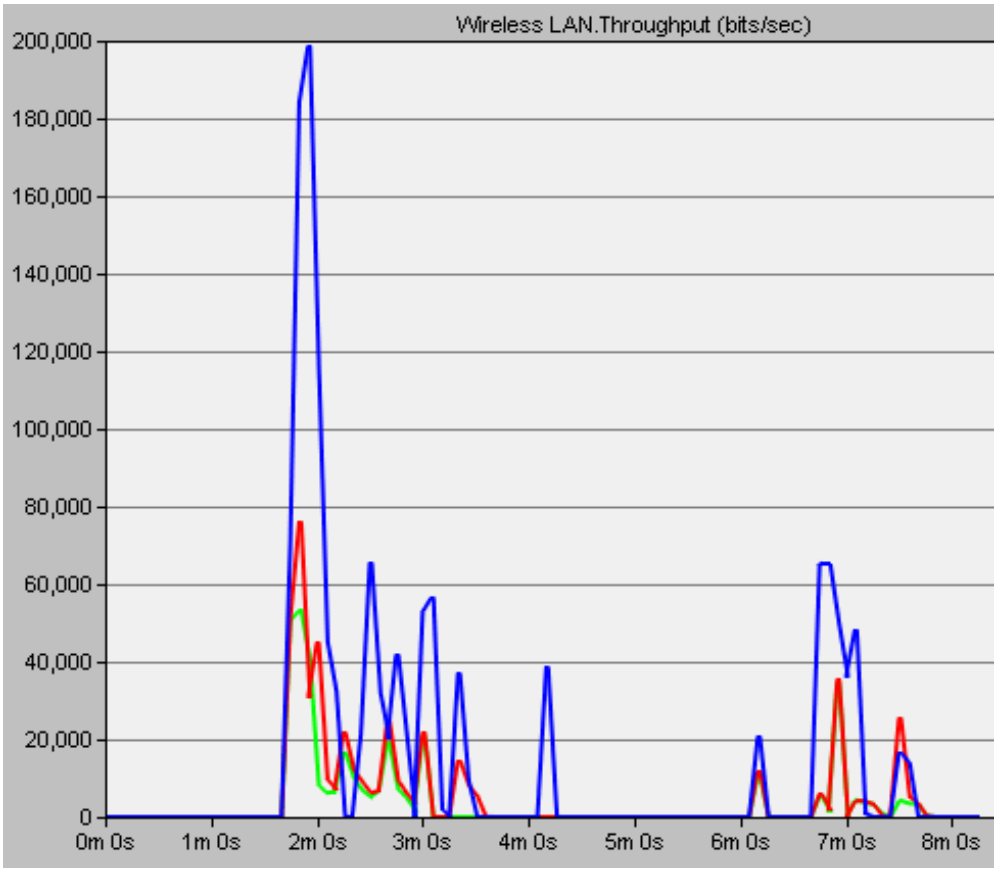

Figure III. Throughput obtained for FTP load with fully co operative nodes (blue), 15% selfish nodes participating in network(red) and selfish nodes not participating in the network.

From figure II and III it is seen that even with 15% selfish nodes in the proposed scenario, the throughput degrades to almost the same levels as of the nodes not participating in the network. Query intensive operations like database applications are more susceptible to degradation compared to FTP loads.

III. CONCLUSION

In this paper we analyzed the performance degradation in an anonymous ad hoc network with selfish nodes under different applications. Simulation was done using 20 nodes with 15% of the nodes being selfish. Similarly the simulation was done with the selfish nodes not participating in the network. As expected the throughput for the given scenario degrades. However the degradation due to 15% selfish nodes is almost equal to the performance degradation if the nodes were not present in the network. Further work needs to be done and throughput evaluated for larger networks.

REFERENCES

[1] R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns inmultihop wireless networks that are not bandwidth limited," Proceedings of IEEE GLOBECOM, pp 2957 – 2961, 2003.

[2] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," ACM SIGCOMM Computer Communication Review, pp 234 – 244, October 1994.

[3] T. Clausen, P. Jaquet, et.al. *"Optimized link state routing protocol"*. Internet Draft, draft-ietfmanet-olsr-06.txt, work in progress, 2001.

[4] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Computing, volume 353. Kluwer Academic Publishers, 1996..

[5] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," Second IEEE Workshop on Mobile Computer Systems and Applications, pp. 90-100, February 1999.

[6] Kimaya Sanzgiri , Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields. A Secure Routing Protocol for Ad Hoc Networks. In 10 Conference on Network Protocols (ICNP), November 2002.

[7] Seung Yi, Prasad Naldurg, Robin Kravets. Security-Aware Ad hoc Routing for Wireless Networks. In Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01), 2001.

[8] P. Papadimitratos, Z.J. Haas, P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. draft-papadimitratossecure-routing-protocol-00.txt 2002-12-11

[9] Jiejun Kong, Xiaoyan Hong, and Mario Gerla, "An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, vol. 6, no. 8, pp. 888-902, Aug. 2007.

[10] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks. In *29th IEEE International Conference on Local Computer Networks (LCN'04)*, pages 618–624, 2004.

[11] R. Song, L. Korba, and G. Yee. AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2005.