EFFECT OF DENSITY ON SECURITY ATTACK IN MOBILE AD HOC NETWORK

[1]JOSHI SHRADDHA D., [2]PROF. INDR JEET RAJPUT

[1]PG Student, M.E. in Computer Engg, Hasmukh Goswami College Of Engineering
[2] Assistant Professor , Computer Engineering, Hasmukh Goswami College Of Engineering

Shr27joshi@gmail.com, Indra.rajput@gmail.com

ABSTRACT: *A multi hop mobile ad hoc network is a peer to peer network of wireless nodes where nodes are required to perform routing activity to provide end to end connectivity among nodes. As mobile nodes are constrained by battery power and bandwidth, some nodes may behave selfishly or maliciously and deny forwarding packets for other nodes, even though they expect other nodes to forward packets to keep network connected. The problem of all the current ad hoc routing protocols is that they trust all nodes and assume that they behave properly; therefore they are vulnerable to attacks launched by misbehaving nodes. The resource limitation of nodes used in MANET, along with the multi-hop nature of this network may cause a new phenomenon which does not exist in traditional networks. To save its resources node may behave selfishly and uses the services of other nodes without correctly participate in system. We simulate forwarding node selfish behaviors on top of Dynamic Source Routing (DSR) protocol: selfish nodes do not forward control packets (routing packets) for other nodes and malicious nodes do not forward data packets of other nodes. We compare the throughput of scenario with selfish nodes and without it and show that the selfish behavior can make network efficient. We also found that in dense mobile ad hoc networks where route breakages are frequent, routing control packets consume significant fraction of bandwidth and selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in lesser collision for both, well behaving nodes and selfish nodes.*

KEY WORDS: *Mobile Ad Hoc Network, DSR, Selfish Behavior, Efficient Network.*

1. Introduction

A Mobile Ad hoc Network is a collection of wireless nodes communicating with each other in the absence of any infrastructure. Due to this infrastructure less feature, all networking functions must be performed by the nodes themselves. Packets sent between distant nodes are expected to be relayed by intermediate nodes, which act as routers and provide the forwarding service. As mention in [1] mobile nodes are typically constrained by power and computing resources, a selfish node may not be willing to use its computing and energy resources to forward packets that are not directly beneficial to it, even though it expects others to forward packets on its behalf.

In this work, we analyze the effect of density on selfish behavior in MANET. We studied various selfish behaviors in literature (Section 2: Related Work) and identified the forwarding node selfish behavior for simulation and analysis: selfish nodes do not forward data or control packets (routing packets) for other nodes. We compare the throughput to the selfish nodes for misbehavior and show that the certain numbers of selfish nodes are good for network and improve throughput. We consider this as an important finding because as per our knowledge almost all the cooperation enforcement mechanisms except PCOM [2] address the forwarding node selfish behavior. Please refer to [1][4][5][6][3][7] for cooperation enforcement mechanisms addressing forwarding node selfish behavior.

Secondly, we find that in dense mobile topology ad hoc networks selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in efficiency enhancement for both, well behaving nodes and selfish nodes. We find that in mobile topology network scenario route caching mechanism of DSR is not effective and every link break results in route request flooding in the network. As in the dense network there are excessive number of nodes participating in route discovery, selfish behavior by certain number of nodes prunes some route discovery paths which in turn reduces the overall congestion of network and increase performance of network.

This paper is organized as follows: section 2 discusses related work; Section 3 is about simulation setup; section 4 presents simulation analysis; and section 5 presents our major conclusions and future work.

2. Related Work

2.1 Selfish Behaviors in MANET

The limitation in resources along with the multi-hop nature of Mobile Ad hoc Networks (MANETs) causes a new vulnerability that does not exist in traditional networks. To preserve its own resource, a node may behave selfishly. We identified following selfish behavior from literature.

Forwarding Node Selfish Behavior [6]: In these selfish nodes do not participate correctly in routing function by not advertising available routes, for example: in DSR selfish node may drop all RREQ they received or not forward a RREP to some destination. Consequently, this selfish node will not participate in the requested routes.

Packet Dropper [8]: One of the commonest threats that mobile ad hoc networks are vulnerable to is data packet dropping, which is caused by selfish nodes. Most of the existing solutions to solve such misbehavior rely on the watchdog technique [1].

Partial Dropping [9]: Selfish node can circumvent the watchdog by dropping packets at a lower rate than the watchdog's configured minimum misbehavior threshold.

Emulate Link Breakage[10]: When source node (R) want to transmit packet to next node (R+1) on certain route R, if R+1 is selfish , R+1 can simply keep silent to let R1 believe that R+1 is out of R1's transmission range.

We simulate forwarding node selfish behavior because it targets forwarding functionality of DSR protocol and most of the research work has been done on this attack. So we need to evaluate whether this behaviors can be beneficial to network or not.

3. Simulation

Simulations have been carried out to in order to analyze the effect of density on selfish behavior on DSR protocol. We simulated this behavior using Ns-2.34 [11][12]. We focused our attention on the evaluation of network performance in terms of routing overhead, throughput and packet deliver ratio of a mobile ad hoc network where a defined number of nodes were misbehaving.

3.1. Forwarding Node Selfish Behavior

In this behavior, Selfish node does not perform packet forwarding function [1][4]. When this behavior is applied, the node disables the packet forwarding function for all packets that have a source address or destination address different from the current selfish node. Node with this kind of selfish behavior does not participate in route discovery phase of DSR protocol and does not forward any data packet.

3.2 Simulation Setup

We conducted exhaustive simulations in the simulation tool NS-2.34[11][12]. We took average of 10 simulations. The number of nodes (network size N) is varying. The mobility model chosen is the Random Way Point Model [13], which is general in nature and provides the uniform node distributions. Unless otherwise indicated, the speed is uniformly distributed between 0 and 20 ms. we used Random Way Point model [13] because we were not targeting particular application. Constant Bit Rate (CBR) Traffic Model is chosen for generating data packets. In each traffic pattern, 50 sessions are constantly maintained to keep every node involved in networking.

The results are averaged of 10 simulation rounds conducted with various random seeds. The simulation time is set to 1000s so that the system can reach steady states. We set maximum number of packet as 10000 for forwarding node misbehavior which is large enough to continue session till end of the simulation time. The default network parameters are listed in Table 1.

General Parameter	
Number of Nodes	10,20,30,40 50,60,70,80
Topology	Mobile
Simulation Time	1000 Sec
MAC Layer	802.11
Range	200 meters
Simulation Area	1000 x 1000 m
Traffic Model	Constant Bit Rate
Packet Size	512 Bytes
Interval	1 Sec

Table 1: Simulation Parameter

4. Observation

4.1. Forwarding Node Selfish Behavior on Dense Mobile Ad hoc Network

Selfish node does not perform packet forwarding function of DSR protocol. Node with this kind of

selfish behavior also does not participate in route discovery phase of DSR protocol.

4.1.1 Throughput

Figure 1 shows the simulating result of dense topology network scenario. Throughput is measured as ratio of total number of packets successfully delivered to destination nodes and total number of packets generated by source nodes. There are two things need to be observed from graph:

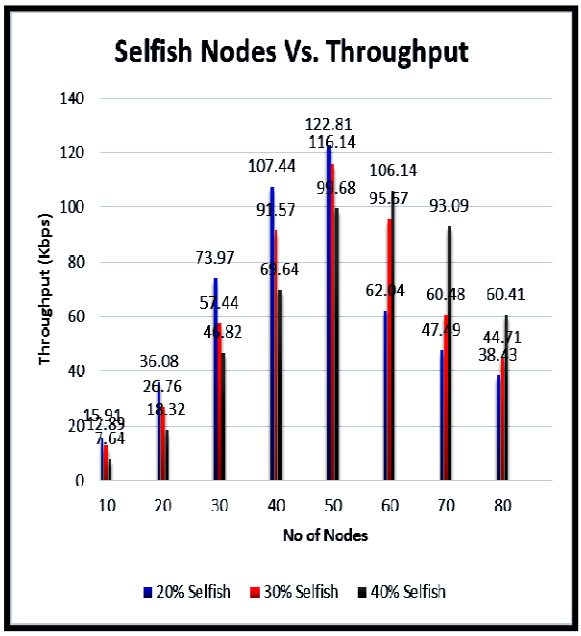

Figure 1: Throughput Analysis

1) In the sparse network i.e. from 10 to 50 numbers of nodes, as number of selfish nodes increase into the network, throughput of network is decreased. This is due to the fact that as more and more nodes behave selfishly, network becomes partitioned and nodes face difficulty in establishing end to end path from source to destination.

2) Whereas in dense network i.e. from 60 to 80 number of nodes, As number of selfish nodes increases in network, the network throughput increases due to reduction in number of collisions. This is due to the fact that as more and more nodes behave selfishly, routing overhead of network decreased and collision will be reduced in network which intern increase network throughput.

4.1.2 Routing Overhead

In mobile topology network scenario, link breakages are frequent and routing overhead is a major component in performance. When node density is high and all the nodes participate in flooding based route discovery, nodes generates more number of routing packets. When some nodes behave selfishly, they prune all route requests coming to them. This behavior reduces routing overhead of network.

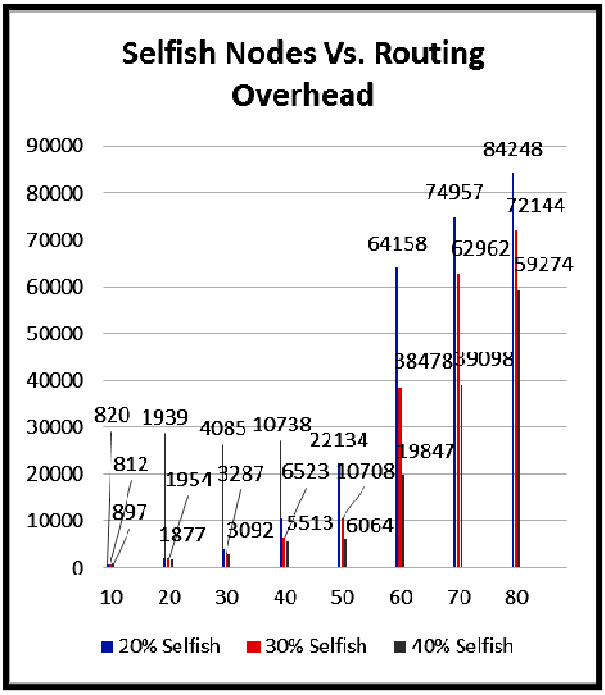

Figure 2: Routing Overhead Analysis

Figure 2 shows that as number of selfish nodes increases in dynamic topology dense network, the routing overhead decreases. Routing overhead is monitored in terms of number of routing control packets in the network. Due to drastic decrease in routing overhead, overall network become efficient and network throughput increases.

4.1.3 Packet Delivery Ratio

In mobile topology network scenario, when node density is high and all the nodes participate in flooding based route discovery, nodes generates more number of routing packets and it creates collisions. When node density is high nodes tend to lose packets because of collision.

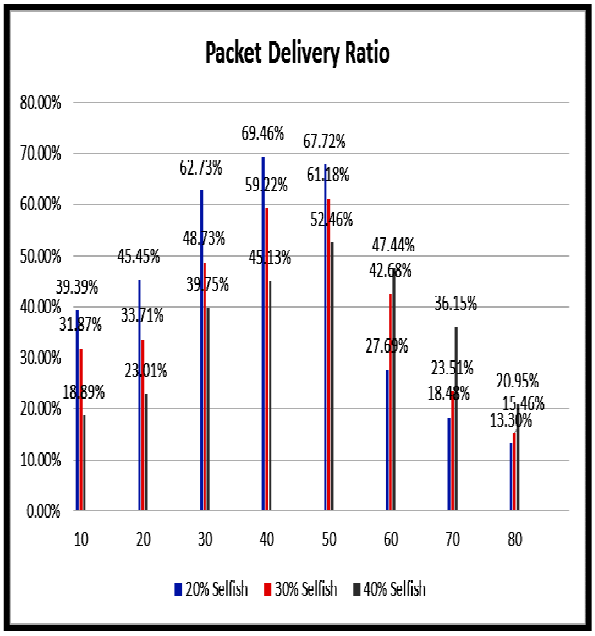

Figure 3 Packet Delivery Ratio Analyses

Figure 3 shows that when some node behaves selfishly, they prune route request and route reply packet which intern reduces the collision of wireless medium. Due to decrement in collision, we are having better packet delivery ratio.

5. Conclusion

In this paper, we simulate forwarding node selfish behavior on top of DSR. We found in the sparse network i.e. from 10 to 50 numbers of nodes, as number of selfish nodes increase into the network, throughput of network is decreased. This is due to the fact that as more and more nodes behave selfishly, network becomes partitioned and nodes face difficulty in establishing end to end path from source to destination. Where as in dense network i.e. from 60 to 80 numbers of nodes, as number of selfish nodes increases in network, the network throughput increases due to reduction in number of collisions. This is due to the fact that as more and more nodes behave selfishly, routing overhead of network decreased and collision will be reduced in network which intern increase network throughput.

Secondly, with our simulation study we find that in dense mobile ad hoc networks where route breakages are frequent, routing control packets consumes significant fraction of bandwidth and selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in lesser collision which increase throughput of network.

6. References

1.Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proceedings of Mobicom 2000, Boston, August 2000.

2.Toshihiro Suzuki, Motonari Kobayashi, Ashiq Khan, and Masanori Morita, "Proactive Cooperation Mechanism based on Cooperation Records for Mobile Ad hoc Networks", IEICE Transactions on Communication, Istanbul, June 2006; Volume E90.

3.P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", In Proc. 6th IFIP Commun. and Multimedia Security Conf., Sept. '02.

4.Levente Buttyan and Jean-Pierre Hubaux,"Enforcing Service Availability in Mobile Ad-Hoc
WANs", 1st IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC 2000), Boston, MA, USA, 11 August 2000.

5.Mandalas, K.; Flitzanis, D.; Marias, G.F.; Georgiadis, P.; "A survey of several cooperation enforcement schemes for MANETs" , Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium on 21-21 Dec. 2005. Athens. pp. 466 – 471

6.Abdelaziz Babakhouya, Yacine Challal, Abdelmadjid Bouabdallah,"A Simulation Analysis of Routing Misbehavior in Mobile Ad Hoc Networks". 2008 IEEE, DOI 10.1109/NGMAST.2008.56.

7.S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad-hoc Networks", Techical Report, Stanford University, '03.

8. Tarag Fahad, Djamel Djenouri, Robert Askwith "On Detecting Packets Droppers in MANET: A Novel Low Cost Approach " in IAS'07 Proceedings of Third International Symposium on Information Assurance and Security.pp.56-64.2007.

9. Djamel Djenouri , Nadjib Badache. Two Hops ack: "New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks". Technical report LSI-TRO704, University of Science and Technology houari boumediene, Algeria, April 2003.

10. Wei Yu and K. J. Ray Liu "Secure Cooperation in Autonomous Mobile Ad-Hoc Networks Under Noise and Imperfect Monitoring: A Game-Theoretic Approach ",IEEE transactions on information forensics and security, vol. 3, no. 2, june 2008.

11..Network Simulator Documentation at http://www.isi.edu/nsnam/ns/

12..Mobility Trace analyzer tools at http://nile.cise.u.edu/important/software.htm

13. .Jungkeun Yoon, Mingyan Liu, Brian Noble "Random Waypoint Considered Harmful'. IEEE INFOCOM-2003.