A NOVEL APPROACH TO ENHANCE ENERGY EFFICIENCY IN DSR PROTOCOL IN MANET

[1] ANIRUDDH FATANIYA , [2] PROF. YASK PATEL

[1] Post Graduate Student, Computer Sci & Engg Dept , Parul Institute of Engg. & Tech
[2] Assistant Professor, Information Technology Dept, Parul Institute of Engg. & Tech

fataniya.ag@gmail.com, patelyask@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 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 data or control packets (routing packets) for other nodes. We compare the energy saving to the selfish nodes for forwarding node misbehaviors and show that the selfish behavior saves energy.

We also found that in dense mobile ad hoc networks where route breakages are frequent, routing control packets consume significant fraction of node energy and selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in energy saving for both, well behaving nodes and selfish nodes.

Keywords: Mobile Ad Hoc Network, DSR, Selfish Behavior, Energy Saving.

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 selfish behavior on energy consumption 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 energy saving to the selfish nodes for misbehavior and show that the selfish behavior saves more energy. 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][14][15] 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 energy saving 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 energy consumption of selfish nodes and other nodes along the pruned path and still keeps network connected.

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 energy 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 battery, 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.

MAC Selfish Behavior[7]: A selfish host can deliberately misuse the MAC (Medium Access Control) protocol to gain more network resources than well behaved hosts. For example, IEEE 802.11 requires hosts competing for the channel to wait for backoff interval before any transmissions. A selfish host may choose to wait for a smaller backoff interval, thereby increasing its chance of accessing the channel and hence reducing the throughput share received by well-behaved stations.

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.

False Misbehavior Accusations[9]: A node may falsely report other innocent nodes in its neighborhood as misbehaving to avoid getting packets to forward.

Insufficient Transmission Power[9]: Selfish node (B) can control its transmission power to circumvent the watchdog. if A is closer to B than C, then B could attempt to save its energy by adjusting its transmission power and makes it strong enough to be overheard by the previous node (A) but less than the required power to reach the true recipient (C).

Imperfect Monitoring[10]: Nodes usually base only on what they have observed to make their decisions, imperfect monitoring can always be taken advantage of by greedy or malicious nodes. For example, when the miss detect ratio is high, a selfish node can always drop other nodes' packets but still claim that it has forwarded.

Set TTL Field to Zero[11]: An effective selfish behavior would be to drop routing packets or forward with a time-to-live (TTL) of 0 so that no paths can be established. A selfish node could thereby avoid forwarding many subsequent data packets.

Increasing Hop Counts[11]: Another selfish behavior would be to make paths that include the selfishly behaving device seem

longer than they really are, perhaps by artificially increasing hop counts so the sources are more likely to choose another routes that appear to be shorter.

Congestion Parameters Modification[12]: A selfish user can disobey the rules to access the wireless channel in order to obtain a higher throughput than the other nodes. A selfish user can also change the congestion avoidance parameters of TCP in order to obtain unfair advantage over the rest of the nodes in the network.

Modification of NAV[12]: A selfish user can manipulate rules of the MAC layer. In 802.11, the selfish node can manipulate the size of the Network Allocation Vector (NAV) and assign large idle time periods to its neighbors, it can decrease the size of Interframe Spaces (both SIFS and DIFS), it can select small backoff values, it can unauthenticated neighboring nodes etc.

Emulate Link Breakage[13]: 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.

Network Card On/Off Misbehavior[2]: A type of selfish behavior which laymen users, without the skills to falsify program codes or data maliciously, are likely to exhibit. This behavior involves refusing to forward any control or data packets for others. Selfish people can take such an action easily, for example by turning the power off or by turning off the communication function when they do not need to communicate.

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 selfish behavior. So we need to evaluate whether this behavior saves more energy compare to other selfish behavior specified in literature.

3. Simulation

Simulations have been carried out to in order to analyze the effect of selfish behavior on network card power function and packet forwarding function of DSR [3] protocol. We simulated this behavior using Ns-2.34 [20][21]. We focused our attention on the evaluation of network performance in terms of routing overhead, throughput and energy consumption 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.

The effect of this selfish behavior in terms of residual energy is that selfish node will save a significant amount of energy as compare to good nodes by dropping data and control packets.

3.2 Simulation Setup

We conducted exhaustive simulations in the simulation tool NS-2.34[20][21]. We took average of 10 simulations. The number of nodes (network size N) is 50. The mobility model chosen is the Random Way Point Model[18], 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 [18] because we were not targeting particular application. Constant Bit Rate (CBR) and Poisson Traffic Model are chosen for generating data packets. We used Poisson traffic [19] because it is more realistic and to make analysis more complete. 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. Physical layer parameters are taken according to wavelan card specification [16][17] . We set initial energy as 1500 Joules which is large enough to continue session till end of the simulation time. The default network parameters are listed in Table 1

General Parameter		**Energy Model Parameter**	
Number of Nodes	50	Transmit Power	1.65 W
Topology	Mobile	Receiving Power	1.40 W
Simulation Time	1000 Sec	Sleep Mode	0.045 W
MAC Layer	802.11	Idle Mode	0.843 W
Range	200 meters	Initial Energy	1500 J
Simulation Area		1000 x 1000 meter^2	
Traffic Model Parameter			
Traffic Model	Constant Bit Rate	Traffic Model	Poisson
Packet Size	512 Bytes	Interval	1 Sec
Interval	1 Sec	Rate	1 Mb

Table 1: Simulation Parameter

4. Observation

4.1. Forwarding Node Selfish Behavior

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 Dynamic Topology with Constant Bit Rate Traffic

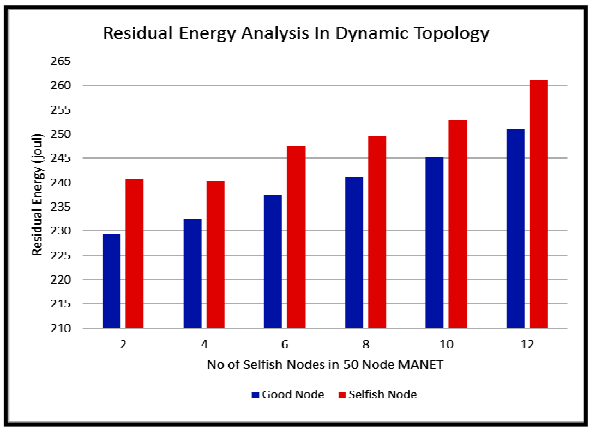

Figure 1 Residual Energy Analysis

Figure 1 shows the simulating result of dynamic topology network scenario. In this scenario as well, good nodes consume more energy than selfish nodes. However the energy saving increases for good nodes as well as selfish nodes as number of selfish nodes increase in network. This is counter intuitive and we identified following reason for it:

In mobile topology network scenario, link breakages are frequent and routing caching mechanism of DSR is not effective. So routing overhead is a major component in energy consumption. When node density is high and all the nodes participate in flooding based route discovery, nodes consume more energy. When some nodes behave selfishly, they prune all route requests coming to them. This behavior saves energy for the selfish nodes and all the other nodes following the node on path towards destination.

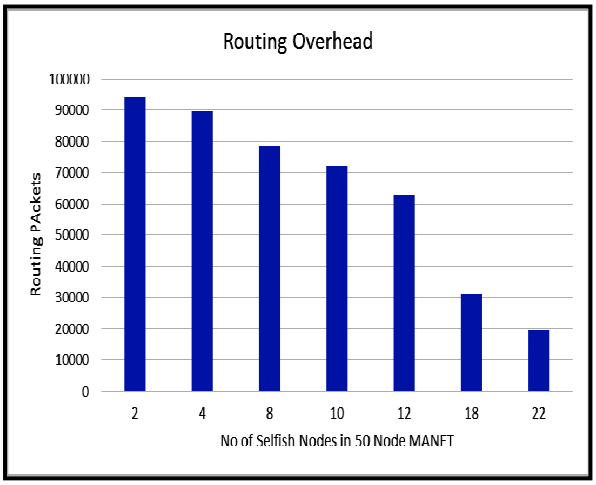

Figure 2 Routing Overhead Analysis

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 good nodes as
well as selfish nodes saves energy.

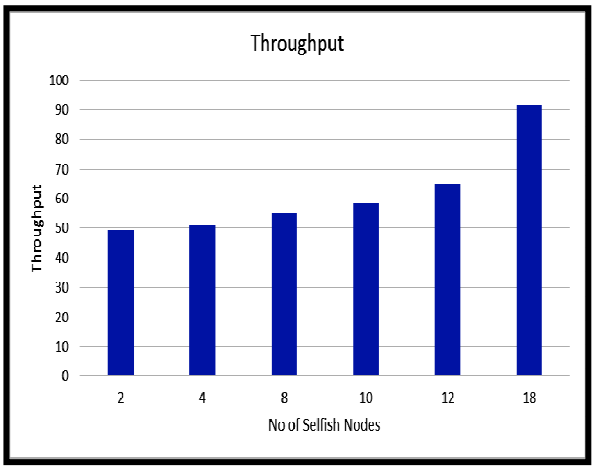

Figure 3 Throughput Analysis

Figure 3 shows the throughput of network with varying number of selfish nodes. Throughput is measured as ratio of total number of packets successfully delivered to destination nodes and total number of packets generated by source nodes. As number of selfish nodes increases up to certain level, the network throughput increases due to reduction in number of collisions. We observe the decrease in throughput after the threshold point (more than twenty selfish nodes in network). 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.

Conclusion

In this paper, we simulate forwarding node selfish behavior on top of DSR. We compare the energy saving to the selfish nodes with good nodes and show that selfish behavior saves more energy. This is very important observation because most of the cooperation enforcement mechanisms proposed in literature addresses the forwarding node selfish behavior.

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 node energy and selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in energy saving for both, well behaving nodes and selfish nodes.

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. David B.,Johnson David A.,Maltz Josh Broch "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless

Ad Hoc Networks", Ad Hoc networking, vol 5, pp 139-172,2001.
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. Lei Guang and Chadi Assi, "Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks,"wimob,pp.116-123,2006 IEEE International Conference on Wireless and Mobile Computing, Networking and Communication,2006.
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. Hyun Jin Kim and Jon M. Peha "Detecting Selfish Behavior in a Cooperative Commons",in Proceedings of IEEE DySPAN,pp. 1-12,2008.
12. A. A. C´ardenas, S. Radosavac, and J. S. Baras, "Detection and prevention of MAC layer misbehavior in ad hoc networks," in Proceedings of the 2nd ACM Workshop on Security of ad hoc and Sensor Networks, SASN, Washington, DC, USA. ACM, 2004, pp. 17–22.
13. Wei Yu, K. J. R. Liu,Attack-resistant cooperation stimulation in autonomous ad hoc networks,Selected Areas in Communications, IEEE Journal on, Vol. 23, No. 12. (05 December 2005), pp. 2260-2271.
14. 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.
15. S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad-hoc Networks", Techical Report, Stanford University, '03.
16. Lucent Technologies. "WaveLan IEEE 802.11 PC Card User's Guide". February, 1999.
17. L. M. Feeney & M. Nilsson `Investigating the Energy Consumption of a Wireless Network Intrface in an Ad Hoc Networking Environment'. IEEE INFOCOM-2001.
18. Jungkeun Yoon, Mingyan Liu, Brian Noble "Random Waypoint Considered Harmful'. IEEE INFOCOM-2003.
19. Andrej KOS, Janez BASTER, "Poisson Packet Generation based on Empirical Data", systmics,cybernetics and informatics, volume-1, number-5,2006.
20. Network Simulator Documentation at http://www.isi.edu/nsnam/ns/
21. Mobility Trace analyzer tools at http://nile.cise.u.edu/important/software.htm