DOI: 10.21917/ijct.2010.0012

PERFORMANCE ANALYSIS OF DSR ROUTING PROTOCOL UNDER ENERGY BASED SELFISH ATTACK IN MOBILE AD HOC NETWORKS

T.V.P.Sundararajan[1] and A.Shanmugam[2]
Bannari Amman Institute of Technology, Sathyamangalam, INDIA
Email: tvpszen@yahoo.co.in[1], dras@yahoo.co.in[2]

Abstract
Mobile Ad hoc Networks (MANETs) rely on the cooperation of all participating nodes to provide the fundamental operations such as routing and data forwarding. However, due to the open structure and scarcely available battery-based energy, node misbehaviors may exist.[1]. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. This paper pointed out Energy based selfish nodes (EBSN) where these selfish nodes tend to use the network but do not cooperate, saving battery life for their own communications [2],[3]. We present a simulation study of the effects of Energy based selfish nodes (EBSN) on DSR routing protocol and its impact over network performance in terms of throughput and delay of a mobile ad hoc network where a defined percentage of nodes were misbehaving.

Keywords:
Cooperation, Selfish Nodes, Ad Hoc Network, Routing

1. INTRODUCTION

An *ad hoc* network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Mobile ad hoc networks (MANET) do not rely on any fixed infrastructure but communicate in a self-organized way.

Security in MANET is an essential component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design [4]. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This very difference is at the core of the security problems that are specific to ad hoc networks. As opposed to dedicated nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions.

If tamper-proof hardware and strong authentication infrastructure are not available, the reliability of basic functions like routing can be endangered by any node of an ad hoc network [5]. No classical security mechanism can help counter a misbehaving node in this context. The correct operation of the network requires not only the correct execution of critical network functions by each participating node but it also requires that each node performs a fair share of the functions. The latter requirement seems to be a strong limitation for wireless mobile nodes whereby power saving is a major concern. 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. According to [6], [7],[8] nodes misbehave because they are *malfunctioning, selfish* or *malicious*.

Selfish nodes can agree to forward packets on behalf of other nodes but silently drop the packets in attempt to save their resources (energy and bandwidth). Malicious nodes may try to sabotage other nodes or even the whole network, for example one malicious node can advertise itself as having the shortest path to all nodes in the network then it can cause Denial of Service (DoS) by dropping all the received packets, in *Black hole attack*, or selectively dropping packets in *Gray hole attack*. Even more, malicious nodes can cause sever damage by collaborating in the attack, such as *wormhole attack*. Several ad hoc routing protocols attacks [9], [10] have been discussed in the literature. However, as far as we can say, there is not a deep study of the impact of such attacks on the performance of routing protocols through simulations.

To address this concern, several secure routing protocols have been proposed recently [11] [12] [13] [14]. Some of these protocols handle attacks by malicious nodes but not the energy based selfish nodes. At the best of our knowledge, there is no solution that handles all misbehaving nodes actions. We think that it is necessary to provide a simulation study that measures the impact of selfish nodes in order to provide protocol designers with new guidelines that help in the design of fault / attack tolerant routing protocols for MANETs.

In this paper, we give a simulation study of energy based selfish nodes impact on DSR [15], [16] performance. First of all, we present an overview of DSR in section 2. Then, in section 3, we give details on our *Energy based selfish nodes* (EBSN) model that include selfish behavior at routing level. In section 4, we describe the simulation environment and methodology in *Qualnet v4.5.* The simulation results were analyzed in Section 5 and finally, Section 6 concludes the paper.

2. DYNAMIC SOURCE ROUTING (DSR)

DSR is an on-demand, source routing protocol. Every packet has a route path consisting of the addresses of nodes that have agreed to participate in the routing of the packet. The protocol is referred to as "on-demand" because route paths are discovered at the time a source sends a packet to a destination for which the source has no path. The DSR routing process includes two phases: the Route Discovery phase and the Route Maintenance phase. When a source node (S) wishes to communicate with a destination node (D) but does not know any path to D, it invokes the Route Discovery function. S initiates the route discovery by broadcasting a ROUTE REQUEST packet to its neighbors that contains the destination address D. The neighbors in turn append their own addresses to the ROUTE REQUEST packet and re-broadcast it. This process continues until a ROUTE REQUEST packet reaches D. D must now send a ROUTE REPLY packet to inform S of the discovered route. Since the ROUTE REQUEST packet that reaches D contains a path from S to D, D may chose to use the reverse path to send back the reply. The second main function of the DSR is Route Maintenance, which handles link outages.

3. TYPES OF SELFISH NODES

Selfish nodes try to save their own resources since resources are very constrained in wireless devices. So selfish nodes may decide to not consume their resource in forwarding data packets for other nodes: this can be achieved in two ways [17]:

Semi Selfish Node (SSN): In the first model, the node systematically does not perform the packet forwarding function which is disabled for all packets that have a source address or a destination address different from the misbehaving node. However, a selfish node that operates following this model participates in the Route Discovery and Route Maintenance phases of the DSR protocol.

The Impact of the Semi Selfish Node (SSN): The consequence of the proposed model in terms of consumed energy is that the SN will save a significant portion of its battery life neglecting large data packets, while still contributing to the network operation.

Fully Selfish Node (FSN): The second model focuses on those nodes that do not participate to the Route Discovery phase of the DSR protocol.

The Impact of the Fully Selfish Node (FSN): The impact of this model on the network operation is more significant than the first one. Indeed, if the node does not participate in the Route Discovery phase, then there will be no route including that node in the path: the consequence is that the packet forwarding function will never be executed. A SN of this type uses the node energy only for its own communications.

Energy Dependent Selfish Node (EDSN): In this proposed model, the node behavior follows the energy levels probed by the node. We propose a selfishness model that uses two energy thresholds (T_{h1}, T_{h2}) to determine the node behavior. When the node's available energy falls within the interval (E, T_{h1}) the node behaves properly, executing both the packet forwarding and the routing function (E corresponds to the initial available energy of the node). When the energy level falls in the interval (T_{h1}, T_{h2}) the node will behave as if it was a *Semi Selfish Node (*SSN), thus disabling the packet forwarding functions.

If the energy level is within the interval (T2, 0) then the same behavior as the one described for a *Fully Selfish Node* (FSN) is selected. Whenever a node has no more energy it is possible to set a stochastic recharge phase: within a limited time interval the node's energy is set back to the initial value.Therefore, the average lifetime (*Lt*) of the node can be defined as ratio of Remaining power to the Power consumption rate. Any cooperative node is assumed to turn off its packet forwarding function if its residual energy drops below 1/ *Eth* of initial energy so that it becomes selfish at time *Tselfish* as given below:

$$Tselfish = (1- 1/Eth)\ Lt \tag{1}$$

Where *Eth* is the selfish threshold parameter and *Lt* is the average lifetime of the node.

4. SIMULATIONS SET UP

The proposed selfishness model is implemented using Network Simulator *Qualnet* v 4.5 tool [18], [19]and the simulation parameters are set as per Table.1 . It contains models and modules at physical and data link layers, medium access control protocols, and the ad hoc routing protocols we want to compare DSR. The node movement scenario allows a node to choose its destination and moves towards it at a uniform speed. This is called the random *waypoint* model. When a node reaches its destination it waits for a pause time before choosing a random destination and repeating the process. Communications among randomly selected nodes are established using constant bit rate (CBR) traffic.

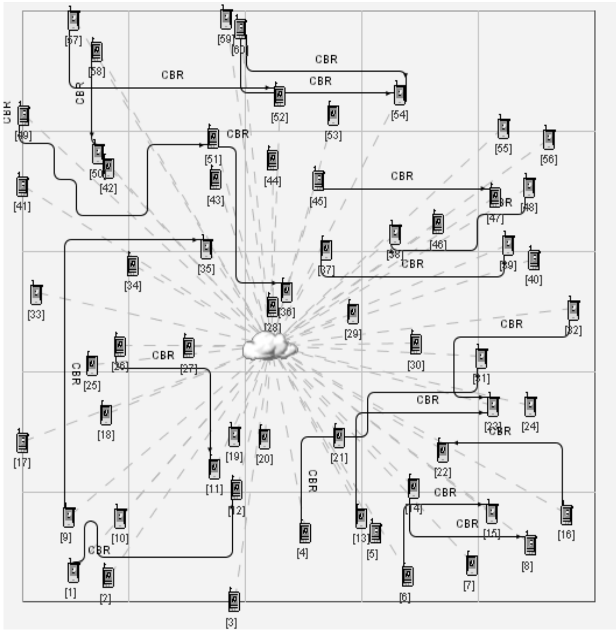

Fig.1. Snapshot of High density network (60 nodes)

5. SIMULATION RESULTS AND ANALYSIS

The topology with 100 nodes is simulated with parameters such as initial energy; traffic load and selfish-threshold parameter set to initial values and their performances are recorded. Selfish threshold (*Et_h*) is varied from 2 to 10; initial energy is set to 1000 and 500 joules; and the results are compared. Simulations are done for seven different random topologies and the average values have been taken for comparison. Fig. 2 portrays the comparison of packet delivery ratio (PDR) with different parameter setting. The consolidated results show that higher initial energy is able to deliver more packets compared to lower initial energy. For a single traffic load, as selfishness of the node increases, packet delivered by the network correspondingly decreases.

There is a heavy packet loss due to network congestion apart from our simulated packet drop due to selfishness. For example, at initial energy=1000, Et_h =10, PDR is maintained more than 99% till traffic becomes medium, but when node density increases to high, PDR comes down to 96%. Due to congestion, about 3% packet loss has occurred, though the environment (i.e. Et_h =10) is more selfless.Fig.2.a shows the performance when the initial energy ($E_{initial}$) of the mobile nodes is set to 1000 joules whereas Fig. 2.b compares the performance if the energy is reduced to 500 joules. PDR drops to 20% on worst-case scenario, where Et_h =2, initial energy ($E_{initial}$) is set to 500 units.

The impact of selfishness on the average end-to-end delay is displayed in Fig. 3 under different initial energy conditions. Having the selfishness of nodes is set to low, the average end-to-end delay increases till the number of nodes becomes 20 and then it starts decreasing. This is due to the fact that the packet loss is more after traffic load crosses the medium level of congestion. Also average end to end delay is defined as the average delay between the sending of data packet by the CBR source and its receipt by the corresponding receiver. This includes all delays caused during route acquisition and buffering at intermediate nodes.

Fig. 3.a shows the average end-to-end delay when the mobile nodes are less selfish whereas Fig. 3.b shows the delay when the nodes are highly selfish.Fig. 4 shows the results obtained simulating a MANET where the EBSN selfishness model was applied to all the nodes of the network pointed out that network performances severely degrade, but the most interesting result has been depicted in Fig. 4. The last family of simulations showed an interesting characteristic of the global network throughput. It has already been showed [20] that the global network throughput decreases when the node mobility increases: the reason is that link outage becomes more frequent causing a higher packet loss probability. On the other side, when every node of the network is selfish of EBSN, simulation results indicate that throughput increases when node mobility increases until it reaches its maximum, then it decreases when node mobility increases. We believe that this particular behavior depends on the mobile node topological position in the network.

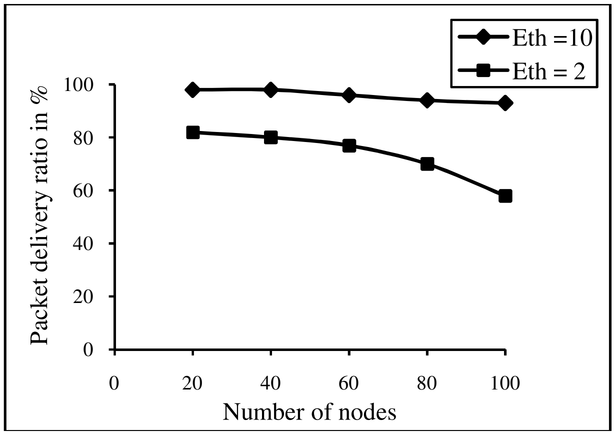

Fig.2.a: Packet delivery ratio for initial energy *EInitial* =1000units

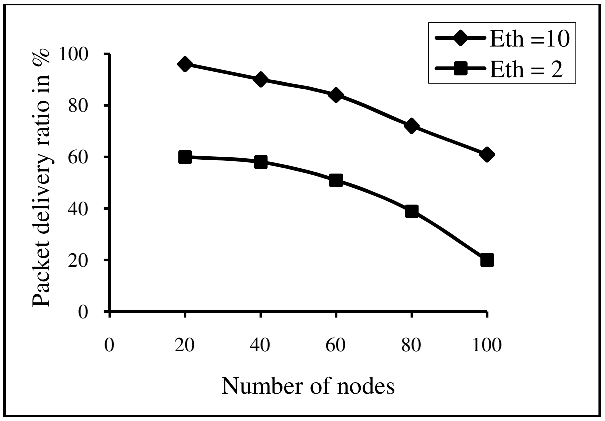

Fig. 2.b: Packet delivery ratio for initial energy *Einitial* = 500units

Fig.2. Packet delivery ratio on initial energy, selfish threshold parameter and node density

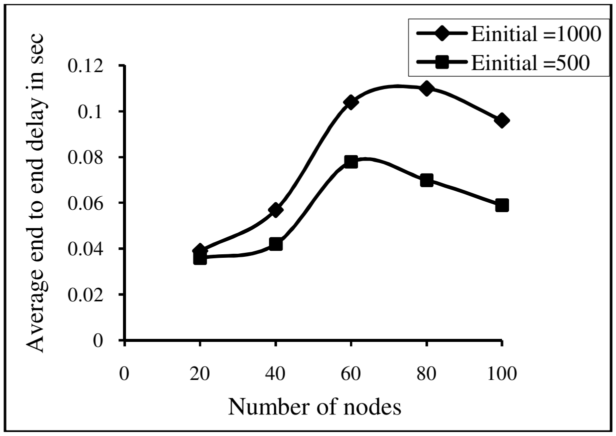

Fig. 3.a: Average end to end delay for selfish threshold *Eth* =10

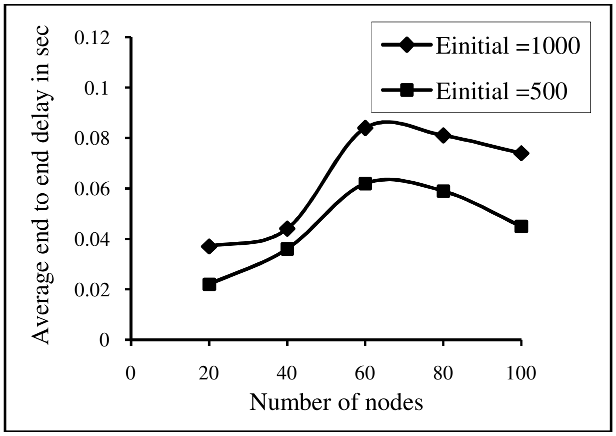

Fig. 3.b: Average end to end delay for selfish threshold *Eth* = 2

Fig.3. Impact of selfishness on average end-to-end delay

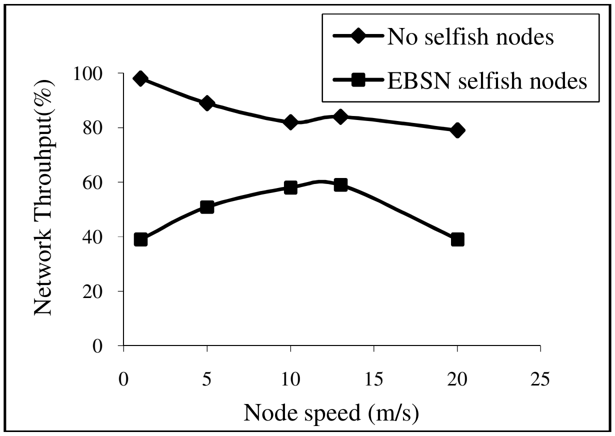

Fig.4. Global Network Throughput vs Node Speed

Given that the communication pattern used in the simulation produce a dense traffic, a central node (i.e. a node that has a central position in the MANET) consume more energy than a peripheral node because it acts as relays for other nodes, wasting its energy for routing and packet forwarding. When mobility is low, all nodes located in a central position stay in the central area of the network and consume more energy than peripheral nodes.Energy consumption leads to a selfish behavior: the packet forwarding and the routing functions will not be correctly executed and the network can be partitioned. As it is possible to see in Fig. 4 for a 1m/s speed, the global network throughput is drastically reduced. When node mobility increases, the location of a node changes from a central to a peripheral position and vice-versa with a high rate, implying that the energy consumption will be equally distributed among the nodes. The selfish behavior is mitigated and throughput increases considerably. However, when the node mobility reaches higher values the influence of the link outage over throughput is more important than the impact of a selfish behavior: speed affects negatively the network performance for speed higher than 13m/s.

6. CONCLUSION

Selfish nodes presence is one major security threat in MANETs that can affect the performance of the underlying protocols. In this paper, we have studied the selfish nodes impact on MANET performance when DSR routing protocol is used. Through simulations, we have seen how selfish nodes can affect network performance. From the investigations, it is found that model is able to regulate the selfishness based on residual energy. With higher energy, the node is able to contribute more cooperation and as well as more packet delivery ratio. It is necessary that the security scheme adopted to face the selfish behavior of a node have to enforce the execution of both the packet forwarding and the DSR functions. Moreover, we believe that a selfish behavior that selectively disables the packet forwarding or the DSR function is not realistic: it is more likely that the node behavior dynamically changes depending on the node's energy level. Therefore, both data and routing packets need to be secured from selfish and malicious nodes. In future work, we will focus to develop a generic mechanism based on reputation to enforce cooperation among the nodes of a MANET and to prevent passive denial of service attacks due to node selfishness.

REFERENCES

[1] H. Miranda and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks," Proc. Seventh CaberNet Radicals Workshop, October, 2002.

[2] L. Buttyan and J.-P. Hubaux, "Security and Cooperation in Wireless Networks," http://secowinet.epfl.ch/, 2006.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, August, 2000.

[4] C. E. Perkins, E. M. Royer, and S. Das. RFC 3561: Ad Hoc on Demand Distance Vector (AODV) Routing. http://www.ietf.org/rfc/rfc3561, July, 2003.

[5] D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR),"Internet draft, February, 2002.

[6] L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," Proc. MobiHoc, August, 2000.

[7] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June, 2002.

[8] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof,Credit-Based System for Mobile Ad-Hoc Networks," Proc. INFOCOM, March-April, 2003.

[9] Barbir, S. Murphy, and Y. Yang. Generic Threats to Routing Protocols. RFC 4593 (Informational), October, 2006.

[10] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pp. 85–97, 1998.

[11] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring.,"Modelling incentives for collaboration in mobile ad hoc networks", 1st Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks", INRIA Sophia-Antipolis, France, 2003.

[12] S. Eidenbenz, G. Resta, and P. Santi, "COMMIT: A sender-centric truthful and energy-efficient routing protocol for ad hoc networks with selfish nodes", IEEE Intl. Parallel and Distributed Processing Symposium- Workshop, Denver, 2005.

[13] S. Bansal, M. Baker, Observation-based cooperation enforcement in ad hoc networks, Technical Paper, Computer Science Department, Stanford University, July 2003.

[14] S. Zhong, J. Chen, Y. R Yang, Sprite: A simple, cheatproof credit based system for mobile ad hoc networks, in: Proc. IEEE INFOCOM 2003, San Francisco, CA, United States, 2003, pp. 1987-1997.

[15] Dave B. Johnson and David A. Maltz., "The dynamic source routing protocol for mobile ad hoc networks", Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, 1999. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[16] D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728 (Experimental), February, 2007.

[17] P. Michiardi and R. Molva. Simulation-based analysis of security exposures in mobile ad hoc networks. *European Wireless Conference*, 2002.

[18] David oliver jorg(2003)“Performance comparison of MANET Routing Protocols in different environment”, IEEE, pp. 1-6, 2003.

[19] Scalable Network Technologies, "Qualnet simulator", Software Package, 2003 [Online].http://www.scalable-networks.com

[20] Josh Broch, David A. Maltz, David B. Johnson,Yih-Chun Hu, Jorjeta Jetcheva, *A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols*, Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking,ACM, Dallas,TX, October 1998.