IMPACT OF SELFISH NODE CONCENTRATION IN MANETs

Shailender Gupta[1], C. K. Nagpal[2] and Charu Singla[3]

[1]Department of Electronics Engineering, YMCA University, Faridabad, India
shailender81@gmail.com[1]
[2]Department of Computer Engineering, YMCA University, Faridabad, India
nagpalckumar@rediffmail.com
[3]Department of Electronics Engineering, NGF College of Engg. & Technology, Palwal,
Charu.singhla@gmail.com

ABSTRACT

The communication in Mobile Ad hoc Network (MANET) is multi-hop in nature wherein each node relays data packets of other nodes thereby spending its resources such as battery power, CPU time and memory. In an ideal environment, each node in MANET is supposed to perform this community service truthfully. However this is not the case and existence of selfish nodes is a very common feature in MANETs. A selfish node is one that tries to utilize the network resources for its own profit but is reluctant to spend its own for others. If such behaviour prevails among large number of the nodes in the network, it may eventually lead to disruption of network. This paper studies the impact of selfish nodes concentration on the quality of service in MANETs.

KEYWORDS

Ad hoc Network, Selfish Nodes, Quality of Service

1. INTRODUCTION

Mobile Ad hoc Networks don't rely on extraneous fixed infrastructure and can be installed without base station and dedicated routers. This makes them ideal candidate for rescue and emergency operations [1] and other short term networks. The nodes in these networks have limited battery power and bandwidth, and each node needs the assistance of others to get its packets forwarded. The conventional protocols in MANETs such as WRP [2], DSDV [3], AODV [4] and DSR [5] assume that all the nodes are cooperative and whenever a node receives a request to relay traffic, it always does so truthfully.

However the experience has shown [6, 7, 8, 9] that as the time passes there is a tendency in the nodes in an ad hoc network to become selfish. The selfish nodes are not malicious but are reluctant to spend their resources such as CPU time, memory and battery power for others. The problem is especially critical when with the passage of time the nodes have little residual power and want to conserve it for their own purpose. Thus in MANET environment there is a strong motivation for a node to become selfish.

Marti et. al [7] have defined the characteristics of selfish nodes as follows:

- *Do not participate in routing process*: A selfish node drops routing messages or it may modify the Route Request and Reply packets by changing TTL value to smallest possible value.

- *Do not reply or send hello messages*: A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it.

DOI : 10.5121/ijwmn.2011.3203

- *Intentionally delay the RREQ packet*: A selfish node may delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths.

- *Dropping of data packet*: A selfish nodes may participate in routing messages but may not relay data packets

The major reason for such behaviour is low residual battery power [6, 8, 9]. It may here be clarified that a selfish node is not malicious and doesn't intend to involve itself in the network damaging activities such as content alteration, spoofing etc. It normally restrains itself from the activities of the other nodes which do not bring any benefit to it.

The literature provides [10, 11, 12, 13, 14] various strategies to deal with such behaviour. These strategies may categorise into two basic categories: Motivation/ incentive based approach and detect and exclude.

The motivation or incentive approach tries to motivate the users of the ad hoc network to actively participate in the forwarding activities. Such a system involves certain amount of money transfer to the relay nodes, on behalf of source or destination, to motivate them to forward messages [11, 15, 16]. One of the motivation/ incentive based approach [8] is based on a virtual currency called nuglet. Every network node has an initial stock of nuglets. Either the source or the destination of each traffic connection use nuglets to pay the relay nodes for forwarding the traffic. The cost of a packet may depend on several parameters such as required total transmission power and the battery status of the intermediate nodes. Packets sent by or destined to nodes that do not have a sufficient amount of nuglets are discarded. The major drawback of this approach is the demand for trusted hardware to secure and maintain the record of the currency at central level. One such protocol, the ad hoc VCG [17] is based on the monetary transfer and discovers an energy-efficient path between the source and the destination. However, the number of messages that must be exchanged in order to find the route to the destination is quite high – in the order of O (n^3), where n is the number of network nodes.

Detect and exclude strategy avoids selfish nodes from the routing paths. This scheme uses two types of trust namely first hand trust and second hand trust.

- First hand trust: The node's personal observation about the neighbouring nodes.

- Second hand trust: The observation communicated by neighbouring node about the other neighbours of the network.

Watchdog and Pathrater [7] is a mechanism based on detect and exclude principle to deal with the selfish nodes. It uses Dynamic Source Routing [18] as base protocol. It has two components: Watchdog and Pathrater. The Watchdog is responsible for detecting selfish nodes that do not forward packets. The Pathrater assigns different rating to the nodes based upon the feedback that it receives from the Watchdog. Each node in the network buffers every transmitted packet for some time. During this interval, the node places its wireless interface into the promiscuous mode in order to overhear whether the next node has forwarded the packet or not and ratings are developed. These ratings are then used to select routes consisting of nodes with the highest forwarding rate.

SORI [22] is a protocol based on detect and exclude mechanism. It makes two record, the local evaluation record (First hand trust) and the overall evaluation record based on the reputation index given by the nodes about their neighbours. Each node in the network maintains tables of first and second hand trust of their neighbouring nodes. Based on these tables the trust of a node is calculated and then action is taken against the selfish nodes

CONFIDANT [19] protocol adds trust manager and reputation index to the Watchdog and Pathrater mechanism. Each node in the network maintains two lists to deal with the selfish nodes. The nodes which behave rationally are kept in the friends list and the nodes which drop the packets or tamper them are kept in the black list. These lists are exchanged by the neighbouring nodes. Based on these list trust of a particular node is calculated. Whenever the trust value for a particular node falls below a certain threshold the protocol stops forwarding packets of that node.

Y. Zhang et. al. [13, 20] designed a intrusion detection system (IDS) for MANETs that consists of Local components: data collection, detection and response and Global components: cooperative detection and global response.

Collaborative Reputation Mechanism (CORE) [21] is similar to the distributed IDS by Zhang et al. and consists of local observations that are combined and distributed to calculate a reputation value for each node. Based on this reputation, nodes are allowed to participate in the network or are excluded. In their work, the authors specify in detail how the different nodes should cooperate to combine the local reputation values to a global reputation and how they should react to negative reputations of nodes. An aspect that is not clearly stated in the work of Y. Zhang et. al.

2. THE CONCEPT AND THE ASSOCIATED WORK

All these strategies are generic and static do not take into consideration the concentration level of selfish nodes into network which may change dynamically. We are of the view that the strategy to deal with this selfish behaviour should be dependent on their concentration level in the network as the impact they have on the network activity will be different at different level of their concentration.

This paper studies the impact of selfish nodes concentration [0-100%] on the various Quality of Service (QoS) parameters [23, 24, 25, 26] related to performance of ad hoc network using MATLAB simulation. The QoS parameters taken into consideration are as follows:

- *Throughput*: Percentage of packets received by the destination to the number of packets sent by the source.
- *Hop count*: Defined as the number of intermediate hops from source to destination.
- *Packet dropped*: Measure of the number of packets dropped by the routers due to various reasons.
- *Probability of Reachability*: Fraction of possible reachable routes to the all possible routes between all different sources to all different destinations.

The purpose of the proposed work is to help the various protocol designers to enable them in incorporating the dynamic strategies to deal with selfish nodes as their concentration varies.

3. SIMULATION AND RESULTS

A simulator was designed in MATLAB in which an area of 30 X 30 sq. unit's size was chosen. In total 40 nodes were distributed randomly in the given area, using *randint* function that uniformly distributes the random numbers, as shown in Figure 1. To create the route between a pair of random source and destination *Dijkstra's shortest path algorithm* was used. To avoid the selfish nodes in the path all the selfish nodes were made unreachable during that particular iteration. Figure 1. shows the snapshot of the simulation process wherein the red lines shows the

shortest path when no node is selfish and the green lines shows the shortest path after the avoidance of selfish nodes. At low concentration of selfish nodes it is more likely green and red lines will be same and as the concentration increases they are likely to be different. Thus at 0% concentration of selfish nodes the route found between a pair of source and destination is shortest and at k% concentration the route found is shortest as if no selfish nodes were present. Thus with the increase in concentration of selfish nodes

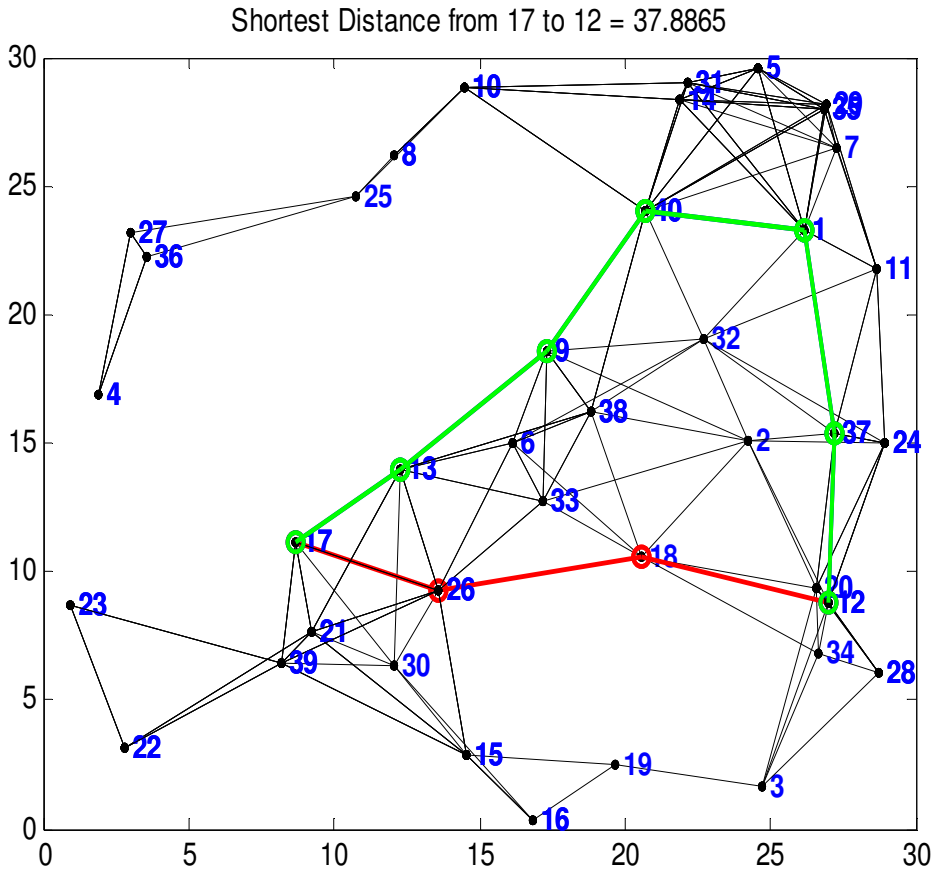

Figure 1. Ad hoc Network

- The average hop count is likely to increase
- The packet drop rate is likely to increase
- The average throughput is likely to decrease
- The probability of reachability is likely to decrease

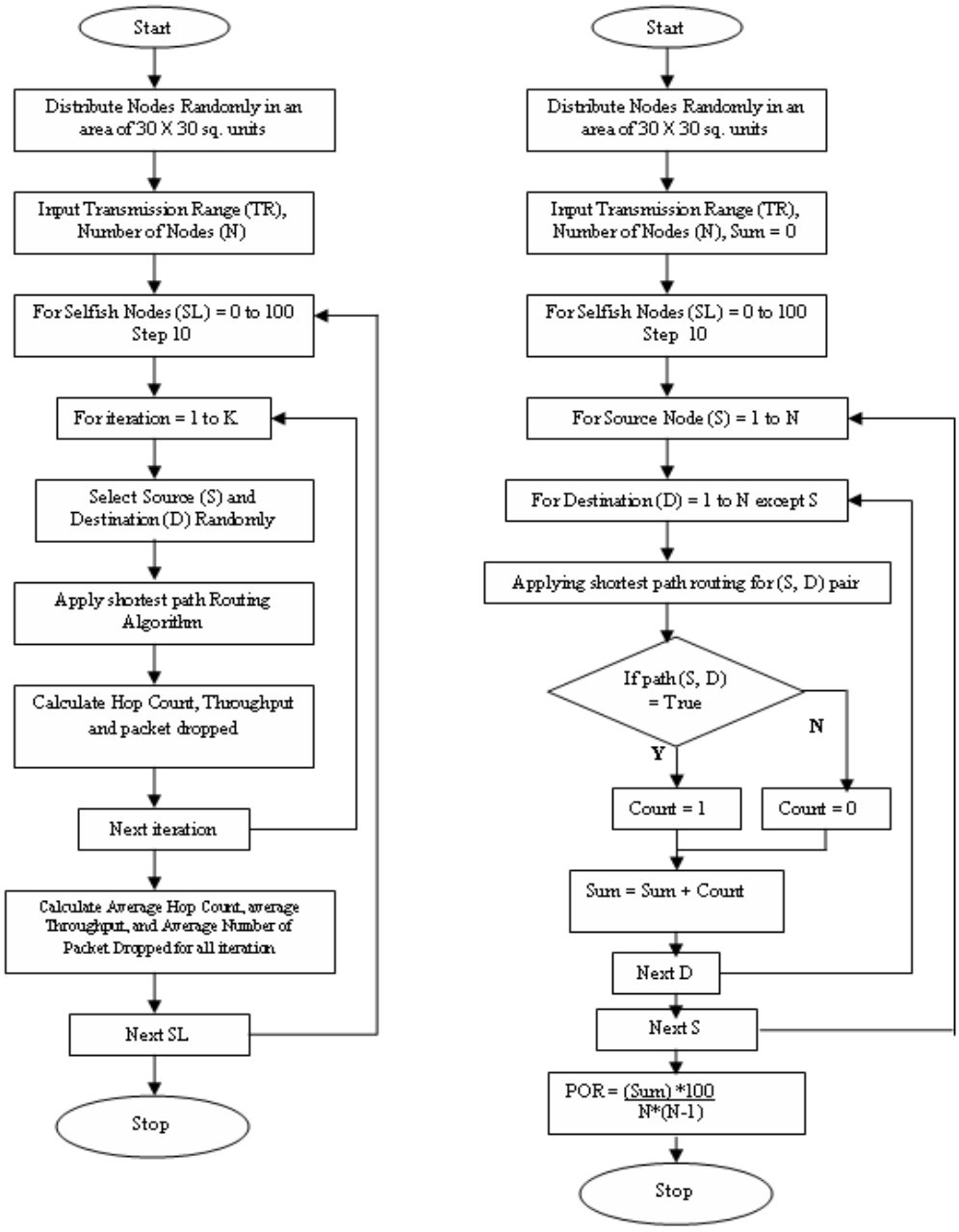

Figure 2. Flowchart of Simulators

Keeping these aspects in view and our simulator tried to make a quantitative assessment of the impact of selfish nodes on the above mentioned QoS parameters. This assessment will enable the designer of the protocols to combat the selfish node problem in the effective manner in an environment where the concentration of selfish node is changing dynamically. The quantitative assessment will enable the designer to make rational decisions while designing the protocol.

Figure 2. shows the flow chart for implementing the simulator on MATLAB.

3.1. IMPACT ON AVERAGE HOP COUNT:

Figure 3. shows the impact of increase in average hop count as the concentration of selfish nodes increases. The average hop count is almost same when the selfish nodes are up to 10% of the total number of nodes. The average hop count increases to 2.5 times when the selfish nodes are nearly 100%. If the route formation does not occour, then in that the maximum hop count (16) was taken.

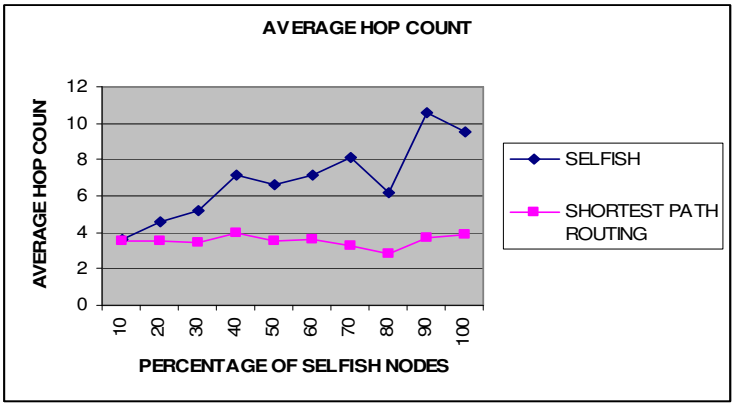

Figure 3. Impact of Selfish Nodes on Average Hopcount

3.2. IMPACT ON NUMBER OF PACKETS DROPPED

Figure 4. shows the impact of selfish nodes concentration on the percentage of packets dropped. There is no remarkable change in the percentage packet dropped when the selfish node concentration is up to 10%. It reaches to a maximum value of nearly 60% when the selfish node concentration is nearly 90%.

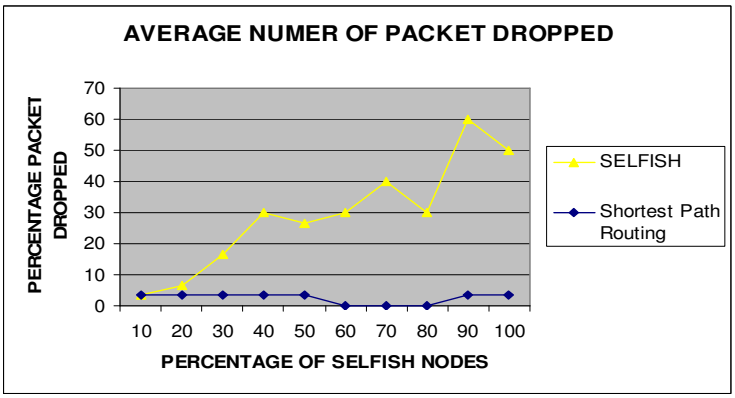

Figure 4. Impact of Selfish Nodes on Average Packet Dropped

3.3. IMPACT ON THROUGHPUT

The results shows that there is no significant decrease in average throughput when the number of selfish nodes up to 10% of the total number of nodes. There is a generic trend of decrease in average throughput with the increase in concentration of selfish nodes. Since the process of source destination pair selection is random there are some fluctuations in the results as shown in Figure 5. It can be seen that the average throughput doesn't fall to zero even if all the nodes are

selfish. The reason for this is that even at 100% selfish behaviour the communication between two immediate neighbours, as source and destination, still survives.

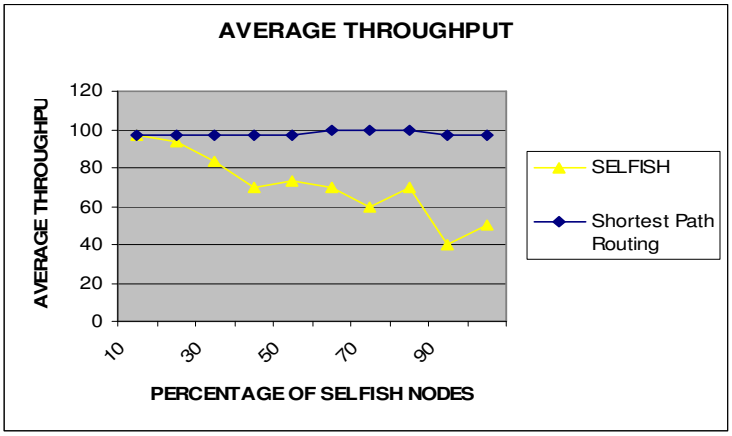

Figure 5. Impact of Selfish Nodes on Average Throughput

3.4. IMPACT ON PROBABILITY OF REACHABILITY

As expected the probability of reachability is nearly 100% when no node is selfish. As the number of selfish nodes increases the probability of reachability decreases but never reaches zero because even at 100% selfish behavior the communication between two immediate neighbors, as source and destination, still survives. Figure 6. shows the impact of selfish node concentration on probability of reachability.

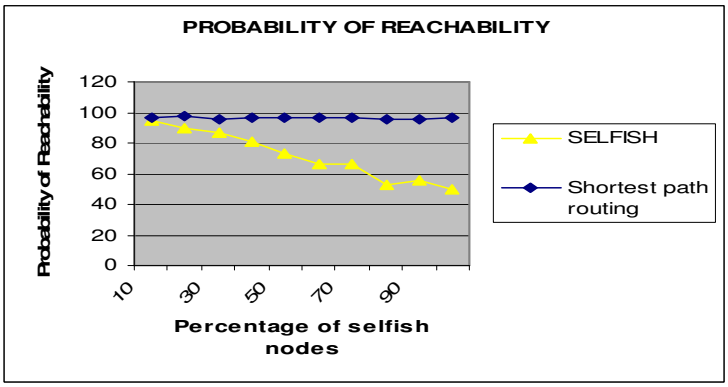

Figure 6. Impact of Selfish Nodes on Probability of Reachability

4. CONCLUSIONS

The problem of selfish nodes is very common in ad hoc networks. The major reason for the selfishness is the loss of power with time. As the time passes away the nodes loose their battery power and in a disaster hit area or battle field area recharging may not be easily possible. The experimental results show that up to a concentration level of 10%, selfish nodes do not have remarkable negative effect on the network activities. As the concentration increases QoS becomes poorer and poorer though the network never comes to halt even if the selfish node concentration reaches to nearly 100%. The average hop count reaches to a maximum 2.5 times, Probability of Reachability and throughput comes down to nearly 50% at its peek and percentage of packet drop goes up to nearly 60% at the most. Since the concentration of selfish

nodes increases with time, the routing protocols can be designed in such a manner that they can react to dynamic change in the concentration of selfish nodes.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1]. Brian B. Luu, Barry J. O'Brien, David G. Baran, and Rommie L. Hardy, "A Soldier-Robot Ad Hoc Network" Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07).

[2]. Murthy, S. and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97.

[3]. C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers," ACM Computer Communication Review, Vol. 24, No.4, (ACM SIGCOMM'94) Oct. 1994, pp.234-244.

[4]. C.E. Perkins and E.M. Royer, "Ad hoc on demand Distance Vector routing," mobile computing systems and applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, 1999, p90 - p100.

[5]. D. Johnson, D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in Mobile Computing (T. Imielinski and H. Korth, eds.), Kluwer Acad. Publ., 1996.

[6]. L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. P. Hubaux, J. Y. Le Boudec, "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes," IEEE Communications Magazine, Vol. 39, No. 6, June 2001.

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

[8]. L. Buttyán, J.-P. Hubaux, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks," Technical report No. DSC/2001/001, Swiss Federal Institution of Technology, Lausanne, January 2001. http://icawww.epfl.ch/hubaux/.

[9]. L. Buttyán, J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," Technical Report No. DSC/2001/046, Swiss Federal Institution of Technology, Lausanne, 31 August 2001. http://icawww.epfl.ch/hubaux/.

[10]. Levente Butty´an and Jean-Pierre Hubaux. Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks. Technical Report DSC/2001/001, EPFL-DI-ICA, January 2001.

[11]. Levente Butty´an and Jean-Pierre Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. ACM/Kluwer Mobile Networks and Applications, 8(5), October 2003.

[12]. Sheng Zhong, Jiang Chen, and Yang Richard Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In Proceedings of IEEE Infocom '03, San Francisco, CA, April 2003.

[13]. Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. In Mobile Computing and Networking, pages 275–283, 2000. also available as http: //citeseer.nj.nec.com/zhang00intrusion.html.

[14]. Yongguang Zhang, Wenke Lee, and Yi-An Huang. Intrusion Detection Techniques for Mobile Wireless Networks. to appear in ACM Wireless Networks (WINET), 9, 2003. also available as http://www.wins.hrl.com/people/ygz/papers/winet03. pdf.

[15]. L. Buttyan and J. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs", in Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, August 2000.

[16]. N. Ben Salem, L. Buttyan, J.P. Hubaux, M. Jakobsson, "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks", in Proc. ACM MobiHoc 03, pp. 13–24, 2003.

[17]. L. Anderegg, S. Eidenbenz, "Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents", Proc. ACM Mobicom, pp. 245–259, 2003.

[18]. D.B. Johnson, D.A. Maltz, J. Broch, et al. DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5:139–172, 2001.

[19]. Buchegger S, Le Boudec JY. Performance analysis of the CONFIDANT protocol. In Proceedings of 3rd ACM International Symposium, on Mobile Ad Hoc Networking and Computing, June 2002.

[20]. Yongguang Zhang, Wenke Lee, and Yi-An Huang. Intrusion Detection Techniques for Mobile Wireless Networks. to appear in ACM Wireless Networks (WINET), 9, 2003. also available as http://www.wins.hrl.com/people/ygz/papers/winet03. pdf.

[21]. Pietro Michiardi and Refik Molva. Prevention of Denial of Service attacks and Selfishness in Mobile Ad Hoc Networks. http://www.eurecom.fr/ michiard/pub/michiardi adhoc dos.ps.

[22]. He Q, Wu D, Khosla P. SORI: A secure and objective reputation- based incentive scheme for ad-hoc networks. In Proceedings of IEEE WCNC2004, March 2004.

[24]. C. Zhu and M. S. Corson, "QoS routing for mobile adhoc networks", IEEE INFOCOM'02.

[25]. C.R. Lin and J.S. Liu, "QoS routing in ad hoc wireless networks", IEEE Journal on Selected Areas in Communications, vol 17, no. 8, August 1999, pp. 1426-1438.

[26]. S. Chen and Klara Nahrstedt, "Distributed quality-ofservice routing in ad hoc networks", IEEE Journal on Selected Areas in Communications, vol.17, no. 8, August 1999, pp.1488-1505.

[27]. Shin Yokoyama, Yoshikazu Nakane, Osamu Takahashi and Eiichi Miyamoto "Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods," Proceedings of the 7th International Conference on Mobile Data Management (MDM'06) IEEE 2006.

First Author Shailender Gupta is B. Tech (Electronics) and M. Tech (Computer Engg.) and pursuing his Ph. D in the area of ad hoc mobile network security. His academic interests include network security, automata theory and fuzzy logic.
Shailender Gupta
Assistant Professor (Electronics Engg.)
YMCA University of Science and Technology, Faridabad
E-mail: shailender81@gmail.com

Second Author Chander Kumar is M. Tech (Computer Engg.) and Ph. D (Computer Science). His academic interests include network security, software reliability and artificial intelligence.
Dr. C.K.Nagpal
Associate Professor.(Computer Engg.)
YMCA University of Science and Technology, Faridabad
E-mail: nagpalckumar@rediffmail.com

Third Author Charu Singhla is B. Tech (Electronics Engg.) and currently pursuing his M. Tech (Electronics). Her academic interests include network security and neural networks and fuzzy logic.
Charu Singhla
NGF College of Engg. & Technology, Vill. Aurangabad, Palwal (Haryana, India)
E-mail: charu.singhla@gmail.com