ZRLBS: Zone Reputation Based Load Balancing Simulator to Grip Selfish Behavior in Social Networks

P.K. Suri[†] and Kavita Taneja[††],

[†]Dean, Faculty of Sciences, Dean, Faculty of Engineering, Professor, Deptt of Comp. Sci. and Applications,
Kurukshetra University, Kurukshetra, Haryana, India.
[††]Asstt. Prof. M. M. Inst. of Computer Technology & Business Management,
Maharishi Markandeshwar University, Mullana, Haryana, India.

Summary
A Mobile Ad hoc Network (MANET) is generally composed of a dynamic set of cooperative neighbors, which are willing to share their wireless transmission power with neighboring Mobile Unit (MU) to support multihop communication between MUs that are not in the direct transmission range of each other. MANETs, blamed of nomadic MUs, limited battery power and unreliable transmission medium, makes them extremely prone to misbehaviors. A relatively less investigated behavioral concern in MANET is caused by the so called cooperative nature of the MUs. Theoretically, MU participation in open communication is crucial leaving no space for issues like preserving the power for personal usage only. Hence, the research effort on MANET focused mainly on routing and assumes that all nodes are usually cooperative. But this a MANET myth, practically limited power and resource constraints can make a MU prone to go into the shell of power save mode resulting in deteriorated MANET performance. This paper summarizes research results addressing the hunting and dealing with selfish behavior in MANETs from a two-side perspective: the detection and punishment of selfish MUs and the proposal of a fairer MANET environment defined by Zone Reputation Based Load Balancing Simulator (ZRLBS) that attempts to split the action area and stochastically leverage the load added to reputation management (creation and maintenance) among the participants MUs to prevent selfish behavior. We evaluated the performance of ZRLBS based scheme using the packet delivery ratio, the communication overhead, and Selfish Node (SN) detection in a discrete event-simulation environment. The results indicate that a reputation-based zone oriented load balancing mechanism can significantly reduce the effect of selfish attacks and improve performance in MANETs.

Key words:
Mobile Ad hoc Network (MANET), Mobile Unit (MU), Selfish Node (SN), Zone Incharge (ZI), Zone Reputation Based Load Balancing Simulator (ZRLBS).

1. Introduction

In MANET, default cooperation assumptions still hold on applications such as military or emergency search and rescue operations, where all MUs belong to the same authority and share the same goals. But the scenario has diversely changed since spontaneous networking grows rapidly with the increase in the interest for mobility and freedom from limitation of fixed communication networks. The today's user rely on mobile computing for a multitude of operations as is equipped with range of MUs like notebook computers, personal digital assistants and other communication hungry portable stuff, with spectrum of wireless interfaces for networked communication [1], thus making MANETs as vital as breathing oxygen in! In this light, MANET is a self organizing and rapidly deployable social ad hoc network in which neither a wired backbone nor a centralized control exists but is definitely the need of the hour to provide anytime anywhere communication. MANET does not have central administration for monitoring behavior of individual MUs, so maintaining the network function for fair MUs when other free riders do not route and forward correctly is a big challenge. This makes it especially crucial to survey selfish misbehavior causes and mechanisms to provide a fair division of tasks in social networks [2]. It is an old proverb that *"Cooperation is induced by equal load in a social community."* In this paper, fair behavior is studied under two harmonizing perspectives: to identify and punish SNs and to enhance existing protocols with ZRLBS based scheme respect to the fair division of tasks. Section 2 discuss about the motivation and types of the selfish behaviors and their possible implications in MANETs. Section 3 deals with related work and presents an exhaustive analysis of the existing selfish behavior prevention schemes in MANETs. Section 4 details the proposed simulator ZRLBS. In section 5, we discuss ZRLBS scheme to detect and prevent selfish behavior in MANETs. Section 6 presents the performance evaluation based on simulation experiments. Finally, Section 7 presents the conclusion and future work.

Manuscript received August 5, 2010
Manuscript revised August 20, 2010

2. Greedy MU in MANET: "MOTIVATION AND FORMS"

Application is the mother of MANET ravenousness. Emerging applications of MANET technology include industrial and commercial applications involving immense mobile data exchange [3]. In addition, open mobile networks can be operated as robust, inexpensive alternatives or enhancements to cell-based mobile network infrastructures. There are also existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks - most of these networks consist of highly-stochastic autonomous topology segments. Generally MUs in MANET have a limited battery life and their residual battery power keeps on decreasing with time [4]. MUs are highly mobile, and this mobility produces effects similar to unit failure, i.e., probabilistic topological changes. There are also wireless sensor applications where dense deployment and significantly larger numbers of nodes are unnecessary, and global IDs are necessary [5]. However, the available energy and memory capacity is highly limited on wireless sensor networks. Detecting routes and forwarding packets eats bandwidth, local CPU time, memory, and energy resulting in a strong motivation for a MU to deny packet forwarding to neighbors, while at the same time using their services to deliver own data [6]. Mobile Computing provide an extremely flexible method for establishing communications for fire/safety/rescue operations or other scenarios requiring rapidly-deployable communications with survivable, efficient dynamic networking. Also, developing technologies of "*wearable*" computing and communications may provide applications for MANET technology. There are likely other applications for MANET technology which are not presently envisioned by the researchers. It is, simply promising efficient IP-based mobile computing for highly stochastic, dynamic and autonomous open networks [7]. But as the needs and users become diverse the lure to conserve and be free riders is becoming more prevalent among MUs. In this scenario, open MANETs will likely resemble social environments: a group of users can mutually benefit from cooperation as long as every person contributes with approximately the *same share*. The categorization of selfish nodes related to MANET routing is presented in this paper as:

Selfish Nodes (SN1) – These nodes participate in the Route Discovery and Route Maintenance phases, but refuse to forward data packets (which are usually much larger than the routing control packets);

Strictly **Selfish Nodes Type 2 (SN2)** – These nodes participate in neither the Route Discovery phase, nor forwarding data packets. They only use their energy for transmissions of their own packets;

Selfish Nodes Type 3 (SN3) – These nodes behave (or misbehave) differently based on their energy levels. When the energy lies between full energy E and a threshold $T1$, the node behaves properly. For an energy level between $T1$ and another lower threshold $T2$, it behaves like a node of type SN1. Finally, for an energy level lower than $T2$, it behaves like a node of type SN2. The relationship between $T1$, $T2$, and E is $T2 < T1 < E$.

Selfish Nodes Type 4 (SN4) - Selfish MU may forward packets with a time-to-live of 0 to prevent path establishment.

Selfish Nodes Type 5 (SN5) - Selfish MU makes the path that include them disguised as longer, by artificially increasing hop counts so the sources are more likely to choose other routes that appear to be shorter.

Selfish Nodes Type 6 (SN6) - Selfish MU manipulate it's transmit power to mislead the *watching* neighbors and getting declared as cooperative nodes.

Often, part of detecting selfish behavior is requiring MUs to watch the transmissions of their neighbors [8]. Selfish behaviors (SN4, SN5, SN6) is not just conserving power by not participating in the routing episode but it goes up to implementing schemes to be spared unnoticed by the selfish behavior detection algorithms.

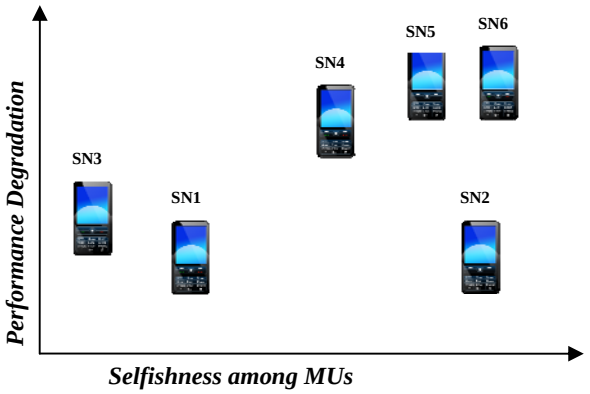

Fig.1 Impact of SNs on performance degradation in MANET.

When MUs know that their behavior is observed by neighbors, they may evade detection by transmitting at a power large enough to be seen by the watchdogs, but too small to be received by the nominal recipient. This paper explores selfish behavior in MANET which is relatively less addressed. Our approach detects selfish behavior that

involves routing protocol packets and not just data packets. Dropped packet is more likely to be retransmitted back leading to a collision thereby preventing the selfish MU from transmitting its own packets too. Dropping a packet once is a one moment benefit but omitting itself from the whole routing episode selfishly can provide a big gain because a MU may avoid subsequent transmission of a potentially large number of data packets for others. Selfish behavior threatens the entire social network. Optimal paths may not be available and cooperative MUs may become overloaded and be forced to abandon the community. The packet drop hinders achieving a secure and reliable communication [9]. SNs, may bring down a functional MANET to a stand still, as the over burdened cooperative nodes lead to the network partitioning. The magnitude of *Selfishness* issue, as shown in Fig. 1 makes it even a higher priority than securing the network because security is needed only when the network is functional to begin with. We argue that as long as the routing algorithm ensures a fair distribution of work among the MUs as each unit is the node as well as the router, selfish behavior can be prevented in a long way.

3. State of Art

MANETs by their very nature are stochastic – in part because of the probabilistic environmental conditions and mobility of the MUs, and in part because of the scarcity and variability of resources especially power and bandwidth. The network topology of a MANET may change frequently and unpredictably. In a MANET, different MUs with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the MUs participate in the network functions. Battery power is considered to be most important in a mobile environment. One of the major sources of energy consumption in the MUs of MANETs is wireless transmission [4]. An individual MU may attempt to benefit from other MUs, but refuse to share its own resources. Such MUs are called selfish or misbehaving units and their behavior is termed as misbehavior [10]. A selfish unit may refuse to forward data packets for other MUs in order to conserve its own power. The misbehavior problem of certain MUs in MANETs has lead to techniques to prevent selfishness in MANETs, broadly classified into three categories [11] reputation-based schemes, credit-based schemes and game theory based schemes. Reputation-Based Scheme [12-18] works on the theme of detection of misbehaving MUs and their boycott from any communication. Each MU participates equally in the absence of any central administration to collectively detect and declare the misbehavior of a suspicious MU. Such a declaration is then broadcasted throughout the network so that the selfish MU will be cut off from the rest of the network. Reputation-Based Scheme [13] contains two major modules, termed watchdog and pathrater, to detect and mitigate, respectively, routing misbehavior in MANETs. MUs operate in a flexible mode wherein the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. Based on the watchdog's labels, the path rater module rates every path and subsequently selects the path that best avoids misbehaving nodes. The drawback is complete reliance on overhearing of a medium that is already mysterious of noise and errors, so it has been found that the watchdog technique fail to detect misbehavior or raise false alarms in the presence of ambiguous collisions, receiver collisions, and limited transmission power. The CONFIDANT protocol [15] is another example of reputation-based schemes. The protocol is based on selective altruism and utilitarianism, thus making misbehavior unattractive. CONFIDANT consists of four important components—the Monitor, the Reputation System, the Path Manager, and the Trust Manager performing the neighborhood watching, node rating, path rating, and sending and receiving alarm messages, respectively. Each MU continuously monitors the behavior of its first-hop neighbor MUs. The misbehavior information is passed to the Reputation System that alters the rating of suspicious MU based on significance and frequency of misbehavior. Once the rating of a MU exceeds the threshold tolerance value, control is passed to the Path Manager, which accordingly controls the route cache. Warning messages are propagated to other MUs in the form of an Alarm message sent out by the Trust Manager. The Monitor component in the CONFIDANT scheme observes the next hop neighbor's behavior using the overhearing technique. The scheme inherits the demerits of the watchdog scheme. The basic idea of credit-based schemes [20, 21, 22, 23] is "serve and earn." Faithful MUs get incentives in terms of virtual currency for providing services to other MUs for efficient communication. When such MUs request other MUs for packet forwarding, the same payment system to pay for such services is implemented. The main hurdle in credit-based schemes is the need of extra protection for the virtual currency and/ or tamper-resistant hardware. Sprite [21] eliminates the use of tamper resistant hardware to stimulate cooperation among the selfish nodes. The need to have a central authority and falling short to consider malicious node's packet drop causes Sprite to be a non-generic proposal. Game theory based [24-27] scheme follow Nash equilibrium including two kinds of games namely Cooperative game in which players reach an agreement through communication and Non-cooperative game in which players chase their own profit independently. GIFT (Generous TIT-FOR-TAT) [24] each MU keeps track of the ratio of services provided to

services taken. But it requires additional information per session leading to overhead.

4. ZRLBS

We propose a simulator for reputation-based scheme for motivating MUs in MANETs to prevent performance degradation due to SNs. ZRLBS give initially warnings before excluding SNs. A MU which becomes indifferent to its reputation and continues to act selfishly can be excluded. If MUs do not cooperate, their reputation gradually decrease and reach a defined threshold, they are eventually eliminated from the network. Also, to avoid discriminating against new incoming MUs in reputation building, the age of a MU is taken into account. Monitoring and preventing selfish activities is challenging in highly stochastic, large MANETs. ZRLBS suggests division of the MANET into small and manageable zones and implement security mechanisms in each zone in a distributed manner. The proposed mechanism involves network split and zone formation, reputation database construction and maintenance, and information exchange. Zones provide a distributed and scalable architecture for network monitoring, reputation data management, and topology control. Zone based architecture also provides a localized detection and prevention mechanism through continuous monitoring and information exchange. This localized and distributed feature also reduces storage and communication overhead, thereby optimizing network bandwidth utilization. For local reputation ratings, data can be obtained from neighbors or a Zone Incharge (ZI) while inter-zonal reputation data can be maintained at the ZI. Later SNs are identified and considered for integration or isolation for smooth communication in MANET.

4.1 Zone based Architecture

ZRLBS make the following assumptions for the proper operation of the proposed scheme:

- MANET is assumed to be composed of homogeneous MUs in terms of computational and storage capability and transmission radius initially, but some resources may vary during the communication process.
- Each MU and ZI in the network has a unique ID and is free to join or leave the network.
- Reputation data exchanged between MUs is truthful and there is no conspiracy among MUs.

ZRLBS use an integrated parameter, which includes the available energy and mobility information for ZI election. A MU is eligible to become a ZI only if it possesses adequate resources, in terms of battery power and lower relative mobility. ZRLBS implements a localized topology control algorithm within a zone and a distributed topology control algorithm among zones. Each zone has a ZI, multiple MUs, and gateways. Each MU knows its neighbors and hello messages are used to maintain connectivity information. A ZI is a MU that manages network content and allows inter-zonal communication. In a zone-based scheme, MANET is treated as a group and each MU is a member that shares common resources. A zone corresponds to a community. As a community member with a good reputation gains respect or incentives to earn better services, while a member with a bad reputation is eventually eliminated from the MANET based on feedback mechanisms.

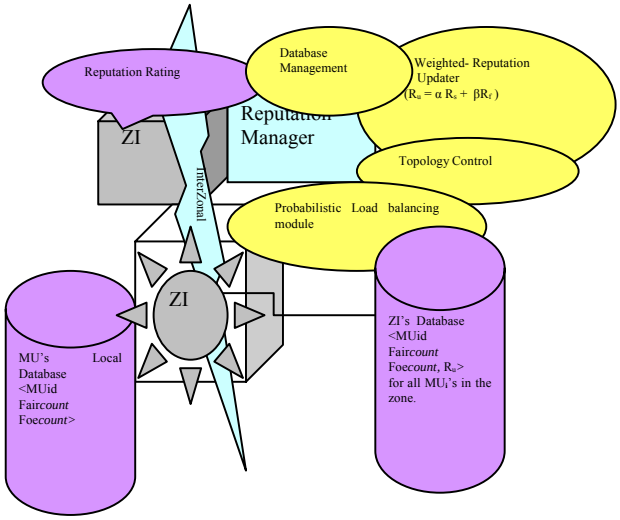

Fig. 2 ZRLBS Architecture

4.2 Reputation Management

The reputation component of ZRLBS consists of four modules for reputation data management and decision making as shown in Fig.2 MUs and the ZI compute and exchange reputation ratings. With this information, a MU can detect a SN and then integrate or exclude it from the MANET. The stochastic topology ruling MANETs imposes the collection of local reputation data without a centralized storage and management facility. ZRLBS aggregates zone wise ratings of MUs. Maintaining all information at each MU congests MANET with system query or reply packets generated by each MU. Aggregating the local reputation data of all MUs in a zone provides a better scope than the neighborhood only information and incurs minimum overhead as compared to global data maintenance. For reputation information exchange, reputation data is collected and maintained at each MU and the ZI in each zone. MUs in each zone

monitor the behavior of their peers and update their reputation data only periodically. Each MU maintains information based on exchange of neighborhood and additional information obtained through a query-reply mechanism. Each MU broadcasts its ratings periodically in a manner similar to a routing information exchange. Each MU maintains a reputation database as <MUid, Fair*count* and Foe*count*> where MUid is the unique IDof each MU, Fair*count* is number of successful services (incremented once for each cooperative act), and Foe*count* is the number of unsuccessful services (decremented once for each selfish act). The reputation database is updated after each service by incrementing/decrementing the suitable counter, according to monitor reports received from others. For a MU to be considered cooperative, its positive reputation rating should be at least equal to its negative reputation. We use data query and reply messages which function as hello messages for the neighborhood communications. The ZI periodically request reputation data from each MU of its zone and broadcast the result to all other ZIs in the MANET. The aim of having the ZI maintain reputation data is to propagate selfish MU information as fast as possible to detect and prevent DoS attacks. Each zone maintains a zonal reputation database as a set of values <MUid, Fair*count* and Foe*count*>.When a MU joins the network; it is given a reputation value of 1. This reputation rating is called an initial threshold. The reputation data is updated based on the MU's own observations as well as information received from peers both for data discovery and exchange mechanisms. Every time this rating is received, a new average is computed with more weight given to the MU's own observation and used further for decision making. Reputation data is also maintained by MU with inter-zonal MUs and intra-zonal information coming from outside ZIs.

4.2.1 Weight-Based Reputation Updates

ZRLBS is built on top of a zone-based architecture where MUs in each zone collaborate in the detection of SN. Forwarding packets originated from cooperative MUs and refusing those generated from SNs can motivate cooperation. To increase the reliability of reputation rating and detect a selfish MU that changes neighbors frequently, weighting was used while updating the reputation ratings. The process gives more weight to MU's own observations and less weight to secondary information. Let R_f be a MU's first hand observed reputation rating and R_s be second hand neighbours' reputation ratings about the same MU. Then, the updated reputation rating (R_u) is computed by Eq. 1.

$$R_u = \alpha R_s + \beta R_f , \alpha, \beta \in [0,1] \text{ where } \alpha > \beta. \quad (1)$$

α and β are configurable parameters and $\alpha+\beta = 1$.

4.3 Load Balancing for long life of Cooperating Nodes (probability distribution)

Each MU normally forwards a packet via a MU with a higher reputation rating. However, such a procedure leads to overloading more cooperative MUs [25]. ZRLBS design attends to load balancing for increasing life of MUs that willingly forward packets to others. Load balancing enables distribution of the network load equally among all potential forwarding MUs. But it assumes a large set of potential cooperative MUs for large networks. We have implemented a probabilistic packet forwarding strategy among eligible MUs based on their reputation ratings. ZRLBS maps the stochastic in MANET by handling the forwarding task probabilistically by choosing the next hop among all candidate MUs. This helps in balancing the load within the MANET while overcoming the effect of packet dropping and selective forwarding.

Load Balancing Algorithm

Step 1 The source MU selects a set (S) of MU with reputation ratings (R) above threshold value (Є) from its neighbors and label them.

Step 2 The source MU sends the packet to a randomly selected MU from the set S: For this Pseudo random numbers are generated and using χ^2 test, we have sample (T) from an exponential distribution with specified expected value $1/\lambda$ as

RN=RNDY1(DUM) (2)

T = -1.0/λ*ALOG(RN) (3)

We generate T_i's according to Eq. 3 and keep on adding them till their sum exceeds 1 and the count gives the Poisson sample (k). MU from set S with label k is selected as next hop for transferring the packet.

Step 3 The process is repeated at all next hops until the packet reaches its destination.

5. ZRLBS Scheme to Grip SNs

MUs in each zone collaborate in the detection of SNs and the prevention of DoS attacks. This is achieved through information exchange at various levels. For DoS attack management ZRLBS scheme as shown below make each MU periodically performs the operations.

ZRLBS Algorithm

Step 1. Computes reputation ratings based on its own observations and second hand information obtained from neighbors and the ZI. If the reputation falls below a predefined threshold, proceed to step 2. Else Step 3
Step 2. Marks the MU as selfish and broadcasts the new reputation rating to all neighbors and to the ZI. All neighbors update their reputation information and decide the status of the MU.
Step 3. Periodically evaluates the reputation information of the MU.
Step 4. SNs are first warned and later excluded if they fail to cooperate in future communications.
Step 5. In addition, if SNs do cooperate, they are re-integrated. But ZRLBS scheme ensures that their packet is not forwarded until their reputation rating reaches a threshold.
Step 6. After SN detection, the information is used to prevent any further occurrence of DoS attacks by forwarding packets via other MUs. (*This can be achieved because each MU maintains multiple routing paths based on reputation ratings*).
Step 7. The reputation threshold values are dynamically selected and adaptive to the network condition.
Step 8. Also ZRLBS scheme ensure load balancing among cooperative MUs with high reputation ratings.

6. Performance Evaluation

The effects on performance of the fraction of SNs, network size, pause time, and simulation time were investigated using the following three major metrics. Packet delivery ratio (defined as the ratio of the total number of data packets received by destinations and the total number of packets sent by a source), SNs detection rate (defined as the ratio of the total number of SNs detected and the total number of SNs in the network) and Communication overhead (defined as the ratio of the total number of routing and reputation related packets and the total number of data packets). We carried out a performance evaluation using NS2 [28].

Table 1 Simulation Parameters

S. No.	*Parameter*	*Value*
1	Simulation Area	1000mx1000m
2	Traffic Source	CBR
3	Routing Protocol	AODV
4	Packet rate	5 packets/s
5	Packet size	128 bytes
6	Number of nodes	70 (max)
7	Number of zones	5-10
8	Transmission range	250 m
9	Simulation Time	1100 s

MUs move according to the random waypoint mobility model and the performance metrics monitored are packet delivery ratio, communication overhead, and SNs detection rate. The effects of SNs on the performance metrics were investigated. The fraction of SNs varied between 0% and 40%. Simulation parameters are shown in Table 1 Simulation results are displayed in Fig. 3-7. The simulation results that show the effect of the fraction of SNs and network size are presented in this section. Fig. 3 shows the packet delivery ratio for SNs. The delivery ratio decreases with the increase in the fraction of SNs with consistently better performance for the ZRLBS scheme. The communication overhead incurred is shown in Fig.4. The results indicate that the overhead slightly increases when the fraction of SNs increases. The transmission and retransmission of route discovery packets and reputation data exchange in ZRLBS scheme results in communication overhead.

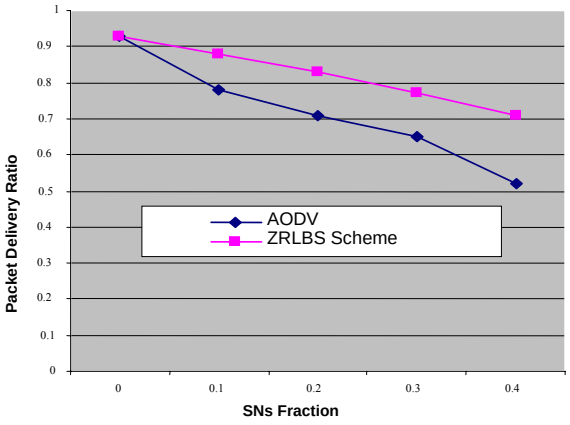

Fig.3 Packet Delivery ratio as a function of SNs

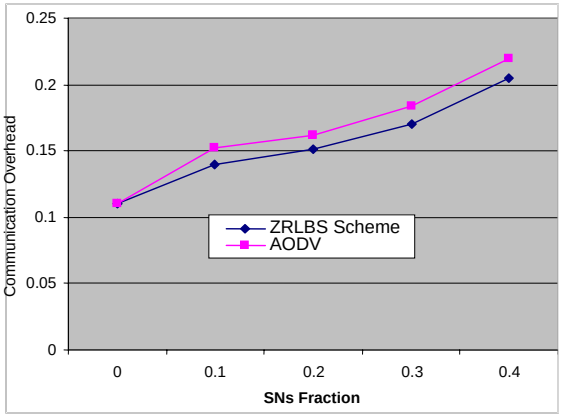

Fig. 4 Communication Overhead as a function of SNs

The simulation results in Fig.7 show that the detection rate of SNs increases from 80% to 99% with Zone based reputation information and from 76% to 96% with neighbor level reputation information. The results show that when zone wise reputation information is used, the probability of detecting SNs faster increases. This is because these can be neighbors with at least one MU and can easily be detected even when mobile. However, as the simulation time increases, the detection rates for both scenarios levels off. Also as shown in Fig. 5 ZRLBS scheme exhibits higher packet delivery ratio compared to AODV as a function of network size. Also an experiment is carried out to determine how long it takes to detect SNs using only neighbor and with zone-based reputation ratings. ZRLBS scheme calculates reputation rating as combined neighbors and ZI reputation ratings.

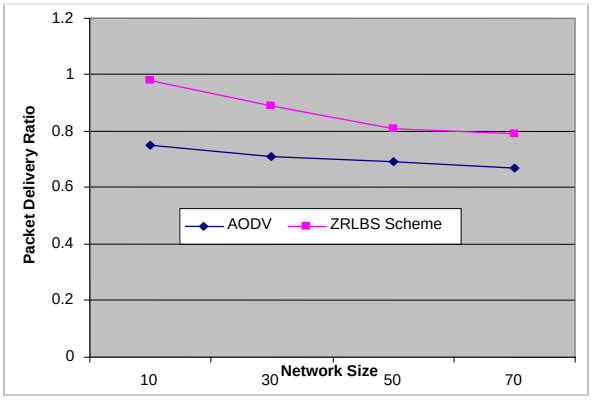

Fig..5 Packet delivery ratio as a function of network size

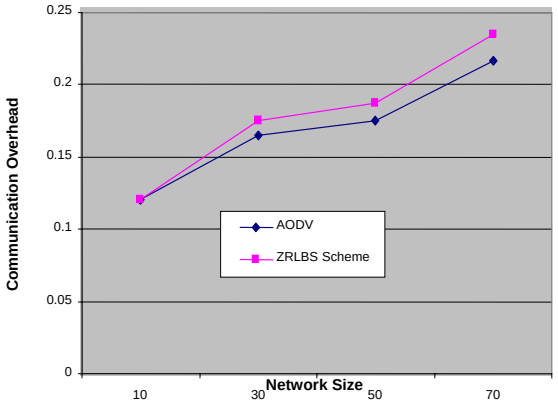

Fig.6 Communication Overhead as a function of network size

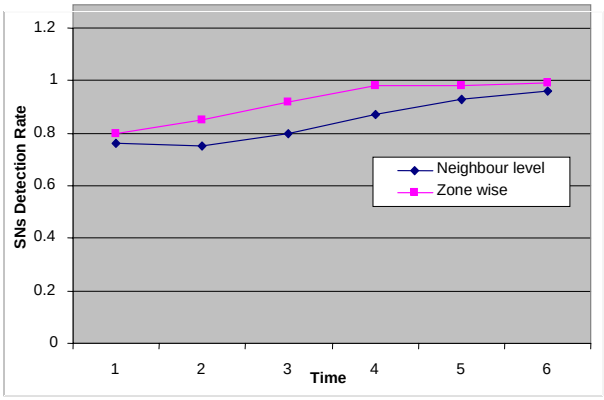

Fig.7 SNs Detection Rate as function of Time

7. Conclusion and Future Work

MANETs as social networks are particularly susceptible to uncooperative behaviors. The generalization of wireless devices has transformed MANETs as the most imperative connection methods to the Internet. In this paper we emphasized that the lack of a common goal in MANETs and absence of a centralized authority make them prone to non cooperation. Each MU will attempt to salvage the most of the network while expecting to pay as less as possible. In human communities, this kind of behavior is termed as selfishness. In this paper the analysis of existing research concludes that complete prohibition of selfishness is impossible over a decentralized network with dynamic topology, applying punishments to SNs may be beneficial. This paper outlines a reputation-based simulator for detecting and preventing selfish behaviors in MANETs. ZRLBS exhibits zone based architecture for performing reputation data management in a localized and distributed manner. Selfish behavior is detected through intrazonal and interzonal monitoring and information exchange. Reputation rating is carried out using neighbour MUs and ZIs information with more weight given to a MU's own observation. ZRLBS scheme is proposed as a bunch of interesting features: its zone wise reputation data creation and management avoids a substantial overhead on the network. Additionally, it is scalable since each MU maintains information about the MUs in its zone only. ZRLBS scheme introduces the concept of "justified selfishness" that makes the whole system fairer, the elimination of SNs from the MANET is not instant as before penalizing each SN is provided with chance to improve its reputation to a threshold. ZRLBS scheme supports an exclusive load balancing mechanism to avoid degradation of cooperative MUs as bottlenecks and then SNs. Stochastics is mapped to probabilistic selections among the candidate intermediate cooperative MUs. We

used simulation to evaluate network performance in the presence of SNs. The simulation results indicate that ZRLBS mechanism is effective in tackling selfish behaviors. The SN detection rate was higher when the zone based reputation rating, as opposed to just neighborhood information, was used. Future work includes the investigation of Distributed Denial of Services (DDoS) in MANET and integrated wireless networks.

References

[1] Greenfield, Everyware: the dawning age of ubiquitous computing, Peachpit Press, Berkeley, CA, USA, 2006.

[2] K. Balakrishnan, J. Deng and P. K. Varshney. "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," in Proceedings of IEEE Wireless Communications and Networking Conference, Vol. 4, pp. 2137- 2142, 2005.

[3] I. Chlamtac, M. Conti, J. Liu, "Mobile ad hoc networking: imperatives and challenges," Ad Hoc Networks, Elsevier, Vol. 1, No. 1, pp. 13-64, 2003.

[4] L.M. Feeney and M. Nilsson, "Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment," in Proceedings of IEEE INFOCOM, 2001.

[5] Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols," Prentice Hall, 2004.

[6] Y. Yoo and D. P. Agrawal, "Why Does It Pay to Be Selfish in a MANET?," IEEE Wireless Communications, Vol. 13, No. 6, pp. 87-97, December 2006.

[7] R. Bruno, M. Conti, and E. Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks," in IEEE Communication Magazine, Vol. 43, No. 3, pp. 123-131, March 2005.

[8] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," In IEEE Security & Privacy, special issue on Making Wireless Work, Vol. 3, No. 3, pp.28-39, June 2004.

[9] V. Balakrishnan and V. Varadharajan, "Packet Drop Attack: A Serious Threat to Operational Mobile Ad hoc Networks," in Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi, pp. 89-95, April 2005.

[10] K. Liu, J. Deng, and K. Balakrishnan, "An Acknowledgement-Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transaction on Mobile Computing, Vol. 6, No. 5, May 2007.

[11] L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad HocNetworks," ACM/Kluwer Mobile Networks and Applications, Vol. 8, No. 5, 2003.

[12] Y. Rebahi, V. Mujica, and D. Sisalem, "A Reputation-Based Trust Mechanism for Ad hoc Networks." In Proceedings of the 10th IEEE Symposium on Computers and Communications, pp. 37-42, 2005.

[13] S. Marti, T.J. Giuli, K. ai, and M. Baker, "Mitigating router misbehavior in mobile MANETs," In the Proceedings of Mobi-Com, pp. 255-265, 2000.

[14] S. Buchegger, C. Tissieres, and J.-Y. Le Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks – How Much Can Watchdogs Really Do?," in Proceedings of the Sixth IEEE Workshop on Mobile Computing Systems and Applications, 2004.

[15] Sonja Buchegger and Jean-Yves Le Boudec, "Performance analysis of the CONFIDANT protocol" in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing'02, pp. 226 – 236, 2002.

[16] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of the 6th IFIP Communications and Multimedia Security Conference, Portorosz, Slovenia, pp. 107–121, September 2002.

[17] H. Miranda and L. Rodrigues, "Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks," in Proceedings of International conference on Distributed Computing Systems, 2003, pp. 440–445.

[18] W. J. Adams, G. C. Hadjichristofi, and N. J. Davis IV, "Calculating a Node's Reputation in a Mobile Ad Hoc Network," in Proceedings of IEEE International Performance Computing and Communications Conference (IPCCC) 2005, pp. 303–307.

[19] L. Buttyan and J. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized ad hoc networks," Technical Report, Swiss Federal Institute of Technology, 2001

[20] L. Buttyan and J. Hubaux, "Enforcing service availability in mobile ad hoc WANs," in the Proceedings of IEEE/ACM MobiHOC Workshop, 2000.

[21] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof,Credit-Based System for Mobile Ad-Hoc Networks," in Proceedings of INFOCOM 03, pp. 1987-1997, April 2003.

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

[23] Y. Yoo, S. Ahn, and D.P. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile MANETs," in the Proceedings of IEEE ICC, 2005.

[24] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini, and R.R. Rao, "Cooperation in wireless MANETs," in the Proceedings of IEEE INFOCOM, 2003.

[25] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan. "Sustaining Cooperation in Multi-Hop Wireless Networks." in Proceedings of the 2nd Conference on Symposium on Networked Systems Design Implementation, Vol. 2, pp. 231-244, 2005.

[26] D. Hales, "From Selfish Nodes to Cooperative Networks – Emergent Link-based Incentives in Peer-to- Peer Networks," in Proceedings of IEEE International Conference Peer-to-Peer Computing 2004, pp. 151–158.

[27] Wei, Hung-Yu, Gitlin and Richard D., "Incentive mechanism design for selfish hybrid wireless relay networks," Mobile Networking and Applications, Vol. 10, No. 6, pp.929--937, Hingham, MA, USA, 2005.

[28] Kevin Fall, Kannan Varadhan: The ns manual, http://www.isi.edu/nsnam/ns/ doc/index.html

Dr. P. K. Suri received his Ph.D. degree from Faculty of Engineering, Kurukshetra University, Kurukshetra, India and Master's degree from Indian Institute of Technology, Roorkee (formerly known as Roorkee University), India. Presently, he is Dean, Faculty of Sciences,
Dean, Faculty of Engineering, Kurukshetra University and is working as Professor in the Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, India since Oct. 1993. He has earlier worked as Reader, Computer Sc. & Applications, at Bhopal University, Bhopal from 1985-90. He has supervised six Ph.D.'s in Computer Science and thirteen students are working under his supervision. He has more than 110 publications in International / National Journals and Conferences. He is recipient of 'THE GEORGE OOMAN MEMORIAL PRIZE' for the year 1991-92 and a RESEARCH AWARD –"The Certificate of Merit – 2000" for the paper entitled ESMD – An Expert System for Medical Diagnosis from INSTITUTION OF ENGINEERS, INDIA. His teaching and research activities include Simulation and Modeling, SQA, Software Reliability, Software testing & Software Engineering processes, Temporal Databases, Ad hoc Networks, Grid Computing and Biomechanics.

Kavita Taneja has obtained M.Phil(CS) from Alagappa University, Tamil Nadu and Master of Computer Applications from Kurukshetra University, Kurukshetra, Haryana , India. Presently, she is working as Assistant Professor in M.C.A. at M.M.I.C.T & B.M., M.M. University, Mullana, Haryana, India. She is pursuing Ph.D in Computer Science and Applications from Kurukshetra University. She has published and presented over 10 papers in National /International Journals/Conferences and has bagged BEST PAPER AWARD, 2007 at International Conference for the paper entitled "Dynamic Traffic -Conscious Routing for MANETs" at DIT, Dehradun. She is supervising five M.Phil scholars in Computer Science. Her teaching and research activities include Simulation and Modeling and Mobile Ad hoc Networks.