A Probabilistic Behavioral Model for Selfish Neighbors in a Wireless Ad Hoc Network

K. Komathy[†], P. Narayanasamy[††],

[†,††]Department of Computer Science and Engineering,
College of Engineering, Anna University,
Chennai, India.

Summary
Some of the challenges in mobile ad hoc networks and sensor networks are the techniques to cope up with selfish behavior of neighboring nodes towards network functions such as routing and forwarding. To devise such techniques it is mandatory to study and analyze the behavior of selfish neighbors under controlled environment and as a result, this paper introduces a probabilistic model that observes the behavior of an intermediary node while forwarding packets for others on a route between a source and a destination. The model formally uses Markov process to represent a cluster of one-hop neighbors as a single collaborative point. From the investigation of the simulated results, it is found that the model is able to regulate the collaboration based on residual energy, the number of neighbors in the cluster, and other network related parameters significantly.
Keywords:
Co-operation, Selfishness, Reputation, Trust, Ad Hoc routing, Markov Chain.

I. Introduction

In wireless ad hoc networks such as mobile ad hoc network and sensor networks, the nodes are dynamically and arbitrarily located in such a manner that end-to-end communication may require routing information via several nodes. Ad hoc network has a variety of security issues, many of which are different from the issues faced by its counterpart, ie. wired network. Since no fixed infrastructure or centralized administration is available, a wireless device has to rely on the neighbors to forward its packets to its intended destination. Compared with wired networks, mobile ad hoc networks are more vulnerable to malicious attacks as well as failures due to their unique features, such as stringent power constraints, error-prone communication media and highly dynamic network topology, which have posed a number of nontrivial challenges to the applications of mobile ad hoc networks. In general, all network functions namely route discovery, packets transfer and network control messages are dependent on the cooperation between nodes.

A mobile node can become a failed node for many reasons, such as moving out of the transmission ranges of its neighbors, exhausting battery power, malfunctioning in software or hardware, or even leaving the network. Besides these failed nodes, based on the behavior, the mobile nodes are classified into:

- *Cooperative Nodes* are active in route discovery and packet forwarding, but not in launching attacks
- *Failed Nodes* are not active in route discovery
- *Malicious Nodes* are active both in route discovery and launching attacks
- *Selfish Nodes* are active in route discovery, but not in packet forwarding. They tend to drop data packets of others to save their energy so that they could transmit more of their own packets and also to reduce the latency of their packets. This type of attack comes under denial-of-service (DoS) category.

Since malicious nodes are considered to be consistently showing the malign behavior, they could be easily identified and isolated from the network using cryptographic techniques. Failed nodes, after recovery, act either as malicious or as cooperative nodes. Behavior of malicious and failed nodes is deterministic and hence, this paper does not include them for study and analysis. Selfish nodes, on the other hand, which cooperate during route discovery and defect during packet forwarding, need to be explored. A behavioral model that could dynamically predict the level of cooperation extended by the node towards the network functions such as routing, network monitoring and packet forwarding is therefore, crucial. In this paper, Markov process is represented to model and analyze the stochastic properties of the node's behavior.

2. Related works

Each node generates traffic for some other node in the network and that the available routes between each source-destination pair are also known. Each source randomly selects one of the possible routes and asks the intermediate nodes on the route to relay traffic. Since energy is a valuable resource, intermediate nodes may not wish to consume their energy to carry the source's traffic. However, if every node behaves selfishly and refuses to cooperate, network throughput may be drastically reduced. Routing protocols for mobile ad hoc network, such as the

Manuscript received July 5, 2007
Manuscript revised July 25, 2007

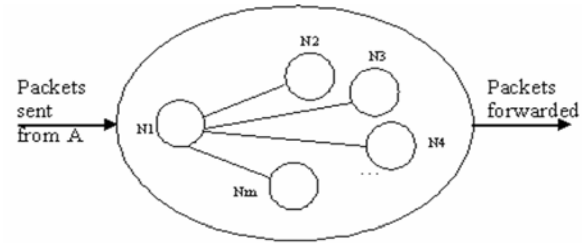
DSR [9], AODV [10], ZRP [11], TORA [12], DSDV [13] are based on the assumption that all nodes will cooperate. These protocols have provided the protection neither for the routing information nor for data. To discourage selfish behavior the technique proposed is through the inclusion of an incentive mechanism that leads to node participation in providing services for others. There are two broad approaches in designing such a mechanism:

- Credit-based: In this approach nodes are rewarded for the services offered. Each node is rewarded with actual or virtual currency for services rendered. This currency can then be utilized in requesting services from other nodes. Mechanisms proposed in [1-5] adopt this approach leading to nodes' sharing their resources in order to gain credit.
- Behavior-based: In this approach nodes are evaluated based on a history of their behavior in the network. Some of the mechanisms which adopt this approach are typically implemented as (i) reputation schemes [6, 7] with each node maintaining a reputation for every other node in the network; or (ii) simple heuristics-based schemes in which the threat of retaliation encourages selfish nodes to cooperate. An example of the latter is the tit-for-tat mechanism in which nodes follow a strategy of mimicking the behavior of their peers [9].

In this paper, the behavior of the selfish neighbors is modeled and the objective is to study the impact of their selfish behavior on the system performance. In particular, it is to analyze the node's behavior while forwarding packets for other nodes. Energy saving is the only reason assumed for a node being selfish. This paper further investigates the tradeoff that exists between energy consumption and the network functions such as packet delivery ratio and average end-to-end delay.

3. Model Design and Analysis

Let us consider a node N1 acting as a next-hop in a route between source A and destination B. Source node then has to depend on N1 for data transfer and if some forecasting and learning mechanism helps the source to make the decision strategy, the data transfer would then be successful. Now, let us examine in this section how this mechanism could be designed and implemented. The node N1 with its one-hop neighbors logically constitutes a union called a cluster. Any two adjacent intermediary nodes say, N1 and N2 within a cluster of one-hop neighbors are generally involved in forwarding each other's packets as illustrated in Fig.1a. This scenario portrays a real-world scenario where one-hop neighbors within a cluster are tightly coupled to each other for successful completion of data transfer and further this bond is extended between clusters or in other words, an optimum level of cooperation between the nodes is essential to carry out the basic functions of the network. Based on the expected level of cooperation represented by the node N1, the performance of the cluster and thereby the performance of the network may be determined.



a) A cluster formed by N1 with its neighbors

b) Probabilistic model representing node N1

Fig. 1. A Dynamic behavioral model representation by Markov process

Markov process helps to characterize the logical representation of a cluster with a single node by its expectant cooperation. Fig.1b shows the dynamic collaborative model represented by Markov process. The probability of cooperation under steady state, p_c shown by the node N1, which depends on its one-hop neighbors, is the expected output from the model. The network selects N1 based on the node's expected cooperation level towards forwarding the packets of others. If p_c is high, the cluster is cooperative and hence it is highly plausible to have high packet delivery ratio; otherwise the cluster is selfish. To make this rational expectation to be factual, the general routing strategy of AODV[10] has been modified to include an additional metric called the expected level of cooperation pertaining to next-hop. Table6 shows a sample of the modified routing table of AODV, which is used in our simulation runs.

3.1. Stochastic properties of a node's behavior :

A random process or a stochastic process is defined to be a Markov process if given the value of X(t), the value of X(v) for v>t does not depend on the values of X(u) for u<t. In other words, the future behavior of the process depends only on the present value and not on the past values. So, a Markov process has a limited historical dependency. A process is said to be Markovian if:

$$P[\, X(t_{n+1}) \leq x_{n+1} \mid X(t_n) = x_n ,\, X(t_{n-1}) = x_{n-1} , \ldots X(t_0) = x_0]$$
$$= P[\, X(t_{n+1}) \leq X(t_n) = x_n]$$

where $t_0 < t_1 < \ldots < t_n < t_{n+1}$ and $X_0, X_1, \ldots X_n, X_{n+1}$ are called the states of the process. If the random process at time t_n is in state X_n, the future state of the random process X_{n+1} at time t_{n+1} depends only on the present state X_n and not on the past states X_{n-1}, X_{n-2},… X_0. The sequence of states {Xn} is called a Markov chain. A node in the proposed model is viewed as having two states namely *Forward* (F) and *Drop* (D) while forwarding packets. A two-state Markov process as shown in Fig.2 is assumed to adequately describe the behavior of the node during forwarding. Let the probability of dropping packets due to selfishness and the probability of forwarding packets due to altruistic nature shown by the node are *a* and *b* respectively and they are independent of each other.

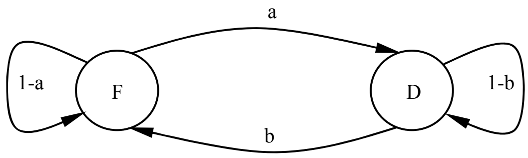


Fig. 2. Two-state transition model representing the behavior of a node

The parameters a and b for the node N1 at time instant k are formally defined as:

$$a = P[\, N^{(1)}_{(k)} = S \mid N^{(1)}_{(k-1)} = C \,]$$
$$b = P[\, N^{(1)}_{(k)} = C \mid N^{(1)}_{(k-1)} = S \,] \qquad (1)$$

during packet forwarding and the two states are represented by {F, D}.

Table 1: Probability transition matrix for a two state Markov chain

State	Forward (F)	Drop (D)
Forward (F)	1-a	a
Drop(D)	b	1-b

Therefore, the behavioral status of the neighbor node i at time instant k is formally given as:

$$N^{(i)}_{k} = \begin{cases} F, & \text{if the level of dropping, } a < \text{Threshold} \\ & \text{and level of forwarding, } b > \text{Threshold ;} \\ D, & \text{Otherwise ;} \end{cases} \qquad (2)$$

At the discrete time instant k, the neighbor node $N^{(i)}$ is in *Forward* state if it is able to forward the packet based on the threshold level at which the node is operating. For example, nodes starting with higher initial energy are expected to forward more packets. Similarly, high altruistic nature will involve in more forwarding action. Referring to Fig.2, let a_1, a_2 be the probability of dropping and b_1, b_2 be the probability of forwarding for N_1 and N_2 respectively. The corresponding probability transition matrices (PTM) for N_1 and N_2 are given in Table 2. With two nodes, the state space occupies four finite states such as {FF,FD,DF,DD} at any point of time. The corresponding finite state Markov chain shown in Fig.3a illustrates the transition probability distribution between different states and the PTM matrix is also given in Table3. The four states $\{S_0,S_1,S_2,S_3\}$ given in PTM are mapped against {FF,FD,DF,DD}. Let π_i denotes the probability of being in steady state. If the state space is finite, then the following set of linear equations can be solved to obtain π_i for $0 \le i \le 4$;

$$\prod \cdot \mathbf{A} = \prod \qquad (3)$$

$$\pi_0 + \pi_1 + \pi_2 + \pi_3 = 1 \qquad (4)$$

where $\prod$ is the probability vector in steady state and A is the matrix representing the transition probability distribution from Fig.3.

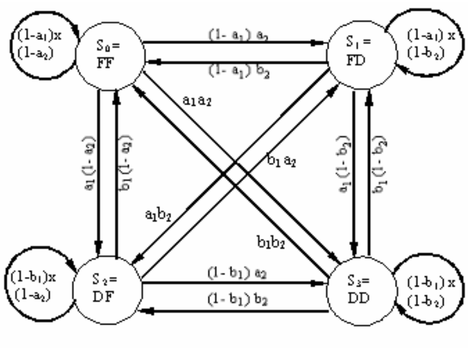
Table 2. Two-state PTM representing neighbor nodes N_1 and N_2

a) node N_1

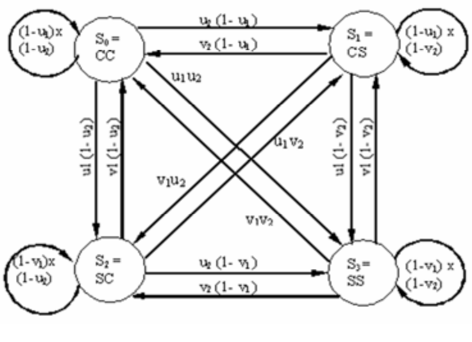
State	Forward (F)	Drop (D)
Forward (F)	$1-a_1$	a_1
Drop (D)	b_1	$1-b_1$

b) node N_2

State	Forward (F)	Drop (D)
Forward (F)	$1-a_2$	a_2
Drop (D)	b_2	$1-b_2$



a)forwarding states between two neighbors



b) cooperation states between a node and its one-hop neighbors

Fig. 3. Finite state Markov chain representing the behavior of one-hop neighbors within a cluster during packet forwarding

Table 3. PTM for four-state Markov chain

	S_0	S_1	S_2	S_3
S_0	$(1-a_1)(1-a_2)$	$(1-a_1)a_2$	$a_1(1-a_2)$	$a_1 a_2$
S_1	$(1-a_1)b_2$	$(1-a_1)(1-b_2)$	$a_1 b_2$	$a_1(1-b_2)$
S_2	$b_1(1-a_2)$	$b_1 a_2$	$(1-b_1)(1-a_2)$	$(1-b_1)a_2$
S_3	$b_1 b_2$	$b_1(1-b_2)$	$(1-b_1)b_2$	$(1-b_1)(1-b_2)$

The status of cooperation involving two nodes N1 and N2 using the four-state packet forwarding function at time instant k is given by the following condition:

$$N^{(1,2)}{}_k = \begin{cases} C, & \text{if } N^{(1)}{}_k = F \text{ and } N^{(2)}{}_k = F; \\ S, & \text{Otherwise}; \end{cases} \qquad (5)$$

The model cooperates and forwards the packets if both nodes are in {F,F} state at time instant k; in all other states, the model represents selfish attitude where the packets will get dropped. The four-state transition given in Fig.3a can be reduced to a two-state where $N^{(i)}{}_{(k)}$ can be modeled with parameters (u_1,v_1) that are defined as:

$$\begin{aligned} u_1 &= P[\, N^{(i)}{}_{(k)} = S \mid N^{(i)}{}_{(k-1)} = C] \\ v_1 &= P[\, N^{(i)}{}_{(k)} = C \mid N^{(i)}{}_{(k-1)} = S] \end{aligned} \qquad (6)$$

From Fig.3a, it is seen that:

$$u_1 = 1- (1-a_1)(1-a_2) \qquad (7)$$

Then, using Equation (3) and (4), we can obtain v_1 as:

$$v_1 = \frac{P[\, N^{(i)}{}_{(k-1)} = S \mid N^{(i)}{}_{(k)} = C] \quad P[\, N^{(i)}{}_{(k)} = C\,]}{P[\, N^{(i)}{}_{(k-1)} = S]} = \frac{u_1\, \pi_0}{1- \pi_0} \qquad (8)$$

where π_0 is obtained from solving Equations (3) and (4) for the four-state model shown in Fig.3a. Equations (7) and (8) represent the cooperation state of a single pair of neighbor nodes only. As a part of four-state transition, its parameters $(u^{(1,2)}, v^{(1,2)})$ can be represented as per Equation(6):

$$\begin{aligned} u^{(1,2)} &= P[\, N^{(1,2)}{}_{(k)} = S \mid N^{(1,2)}{}_{(k-1)} = C] \\ v^{(1,2)} &= P[\, N^{(1,2)}{}_{(k)} = C \mid N^{(1,2)}{}_{(k-1)} = S] \end{aligned} \qquad (9)$$

As a next step, it is proposed to have an iterative approach to model the cluster with multiple neighbor nodes to logically represent it as a single collaborative point.

Let $M \geq 2$ be the total number of neighbor nodes. In the first iteration, neighbor nodes N1 and N2 into one equivalent node. Then the resulting equivalent node is combined with node N3, and so on, until all M neighbor nodes are combined together to form a single collaborative node. For example, the next iteration considers neighbor N3 in the sequence to model the parameters (u_1,v_1) from Equation (7) and (8) and the status of the combined nodes is shown by the four-state Markov process in Fig.3b. Using the resultant four-state model from Fig.3b and Equation set (9), the parameters $(u^{(1,2)},v^{(1,2)})$ can be written as:

$$v^{(1,2)} = 1- (1-v_1)(1-v_2)$$

$$u^{(1,2)} = \frac{P[\, N^{(1,2)}{}_{(k-1)} = C \mid N^{(1,2)}{}_{(k)} = S]}{P[\, N^{(1,2)}{}_{(k-1)} = C]} \text{ x } P[\, N^{(1,2)}{}_{(k)} = S] = \frac{v^{(1,2)} * \pi_3}{1- \pi_3} \qquad (10)$$

where π_3 is obtained by solving the Equations (3) and (4) for the four-state model given in Fig.3b. This iteration is repeated till the cluster is reduced to a single collaborative point. A two-state Markov model is thus obtained representing the status of the final cluster point as $N^{(1,\ldots,M)}(k)$ at time instant k with the following parameters:

$$\begin{aligned} x &= P[N^{(1,\ldots,M)}(k) = S \mid N^{(1,\ldots,M)}(k-1) = C] \\ y &= P[N^{(1,\ldots,M)}(k) = C \mid N^{(1,\ldots,M)}(k-1) = S] \end{aligned} \qquad (11)$$

Fig.4 shows the transition between the two states, Cooperate (C) and Selfish (S) with probability distribution x and y. Let the steady state probability vector of this two state model be, $Ps = [p_c \;\; p_s]$ where p_c denotes the of steady state probability of being in state C and p_s denotes the steady state probability of being in state S. This vector can be obtained by solving a set of linear equations given by:

$$B.\, Ps = Ps \qquad (12)$$

where B is the resultant probability transition matrix.

$$p_c + p_s = 1 \qquad (13)$$

Solving (12) and (13), we get:

$$p_c = \frac{y}{(x + y)} \quad \text{and} \quad p_s = \frac{x}{(x + y)} \qquad (14)$$

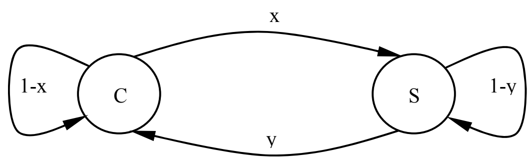
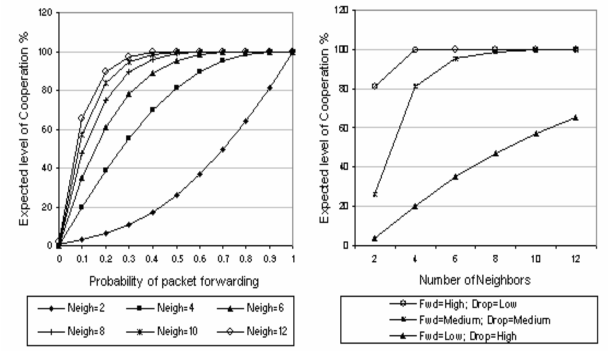


Fig. 4. Final two-state representation of a node with its cluster

3.2. Steady State Behavior:

The system is analyzed under equilibrium state and the performance is illustrated in Fig.5. It is observed from Fig.5a that the convergence of expected cooperation depends on the number of neighbors in the cluster. More neighbors make the convergence faster. The expected level of cooperation is also dependent on the probabilities of forward and drop, which goes as input to the model.

Fig.5b displays the performance at a different perspective. Even the worst-case scenario, having the probability of forward as low and the probability of drop as high, yields 66% of cooperation with maximum neighbors as 12. This value goes down to 3% when the number of neighbors is minimal. The maximum number of one-hop neighbors in a single cluster is arrived as 12 while running the simulation run. The convergence happens even at neighbors=4 when the network is stable.



a) against probability of packet forwarding

b) against the number of neighbors

Fig. 5. Expected level of cooperation under equilibrium state

4. Simulations and Analysis

The proposed behavioral model is implemented using Network Simulator NSv2.28 tool and the simulation parameters are set as per Table5. The simulated topology uses AODV routing with 100 nodes. The performance of network functions such as packet delivery ratio and average end-to-end delay under AODV routing are investigated using the proposed model. Packet delivery ratio is defined as the number of packets delivered at the destination divided by the number of packets sent from the source. Average end-to-end delay is defined as the average delay experienced by a packet to travel between a source and a destination.

Table 5. NSv2.28 simulation parameters

Ad hoc routing	AODV
Number of nodes	100
Topology size	1000 x 1000
Mobility model	Random Way Point
Number of random topologies	7
Number of data sources	5, 10, 15, 20 and 25
Maximum number of packets for each connection	100,000
Packet size	512 bytes
Simulation time	4800sec

4.1. Estimation of Parameters for the Model:

The model design described in Section3 specifies the probabilities of packet drop, 'a' and packet forward, 'b'. Let us now compute these input parameters in terms of network parameters. AODV uses a periodical broadcasting message called HELLO message to update its link information with its neighbors. In the simulated run, a node who initiates a HELLO message is to send the residual energy of the node within the message. Therefore, the average lifetime of the node can be derived from:

$$\overline{L} = \frac{\text{Remaining power}}{\text{Power consumption rate}} \qquad (15)$$

Any cooperative node is assumed to turn off its packet forwarding function if its residual energy drops below $1/\eta$ of initial energy so that it becomes selfish at time $T_{selfish}$ as given below:

$$T_{selfish} = (1 - 1/\eta)\,\overline{L} \qquad (16)$$

where η is the selfish threshold parameter and $\overline{L}$ is the average lifetime of the node. The probability of selfishness, $a = 1/T_{selfish}$ and is given as:

$$a = \frac{\eta}{(\eta - 1)} * \frac{1}{\overline{L}} \qquad (17)$$

$$b = \frac{\text{Number of packets forwarded by the neighbor}}{\text{Number of packets received by the neighbor}}$$

The node is considered to be more cooperative if 'a' tends to be very less, which expects the average lifetime to be very high. Similarly, the probability 'b' can be derived from monitoring the direct trust between the two neighboring nodes in terms of forwarding each other's packets. The measurement is done using a watchdog mechanism, which accounts for the number of packets being maliciously dropped out by the neighboring nodes. This would perhaps decide the level at which the node extends its cooperation. A dynamic cache memory called *Neighbor Table* is used that will periodically register the forwarding rate of the neighbor. Routing table of AODV is also modified to include an additional parameter called the expected cooperation level at steady state from Markov model. The network selects a node based on the equilibrium value p_c from Equation (14). If p_c is high, the cluster is cooperative and hence it is highly possible to have high packet delivery ratio; otherwise the cluster is selfish. Table6 shows a sample of the modified routing table of AODV, which is incorporated in our simulation runs. Routing table updating is normally done whenever HELLO message is broadcasted. Existing routing protocol is well utilized for the purpose of collaboration also. The proposed model, therefore, has imposed only very light computational and storage overheads on the protocol.

Sender nodes are not included in the model as they are always cooperative to transmit their own packets. Similarly, the destination nodes are also not considered as they will never act as defectors. Since forwarding is the most concerned function in a multi-hop network where the throughput depends on how much these selfish nodes cooperate towards forwarding packets, this model monitors only the behavior of these intermediary nodes while forwarding the packets.

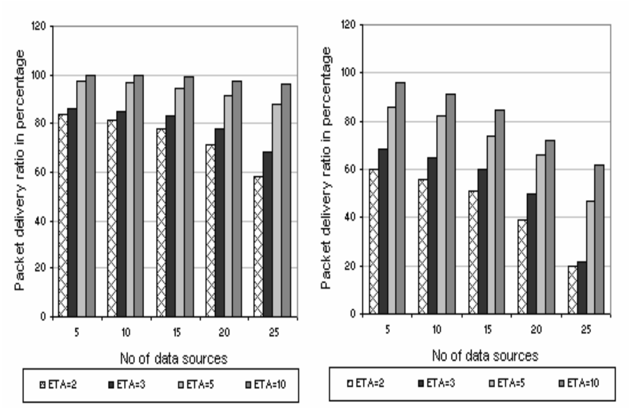
Table 6. Modified routing table of AODV-
Sample Table for Node A @ time t1 seconds

Destination	Seq.No	Hop count	Next Hop	Expected level of cooperation
B	107	3	D	0.87
C	104	5	G	0.21
S	110	2	D	0.45

4.2. Simulation Results and Analysis:

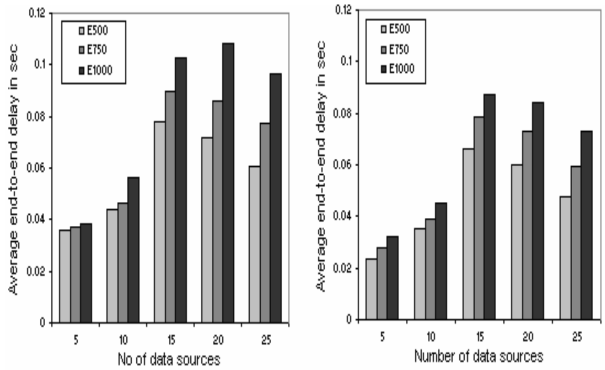
The topology with 100 nodes is simulated with parameters such as initial energy; traffic load and selfish-threshold parameter set to initial values and their performances are recorded. Traffic load is varied from 5 data sources to 25 data sources; η (ETA) is varied from 2 to 10; initial energy is set to 1000, 750 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.6 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.

Generally, the traffic load on the network is classified based on the number of data sources as: high = 20 to 25 data sources; medium = 15 data sources; low = 5 to 10 data sources. The network sustains the load till a medium traffic occurs and yields to heavy traffic. 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, η=10, PDR is maintained more than 99% till traffic becomes medium; but when traffic increases to high, PDR comes down to 96%. Due to congestion, about 3% packet loss has occurred, though the environment (ie.η=10) is more altruistic. Fig.6a shows the performance when the initial energy of the mobile nodes is set to 1000 joules whereas Fig.6b compares the performance if the energy is reduced to 500 joules. PDR drops to 20% on worst-case scenario, where η=2, initial energy=500 units, traffic load=25.



a) Initial energy =1000 units b) Initial energy =500 units

Fig. 6. Dependency of packet delivery ratio on initial energy, selfish-threshold parameter and traffic load



a) selfish-threshold =10 b) selfish-threshold = 2

Fig. 7. Impact of selfishness on average end-to-end delay

The impact of selfishness on the average end-to-end delay is displayed in Fig.7 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 data of sources 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 the average end-to-end delay is computed as:

$$\frac{\sum \text{Time taken by the successfully delivered packets}}{\text{Number of packets successfully delivered}}$$

and therefore, it depends on the packet delivered. Fig.7a shows the average end-to-end delay when the mobile nodes are less selfish whereas Fig.7b shows the delay when the nodes are highly selfish.

5. Conclusion

This paper has proposed a new model, which will learn and predict the behavior of the one-hop neighbors dynamically for maximizing the network functions in terms of collaboration. The model basically represents finite state Markov chain to reduce a cluster of neighbors into a single collaborative point. The model observes the behavior of an intermediary node in a route between a source and a destination, which is a collaborative point of its one-hop neighbors. The performance of the cluster and thereby the performance of the network are dependent on the expected level of cooperation represented by the intermediary nodes. 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. Under steady state conditions, convergence of expected cooperation depends on the number of neighbors in the cluster. More neighbors in the cluster will bring more cooperation.

References

[1] L. Anderegg and S. Eidenbenz., "Ad hoc-VCG: A truthful and cost efficient routing protocol for mobile ad hoc networks with selfish agents", 9th Annual Intl. Conf. on Mobile Computing and Networking San Diego, 2003.

[2] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in self organizing ad hoc networks", ACM Journal on Mobile Networks and Applications(MONET). vol.8, pp.579-592, 2003.

[3] 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.

[4] 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.

[5] S. Zhong, J. Chen, and Y. R. Yang., "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks", IEEE INFOCOM, San Francisco, 2003.

[6] S.Buchegger and J. Y. L. Boudec., "Performance analysis of the CONFIDANT protocol: cooperation of nodes – fairness in dynamic ad-hoc networks", 3rd ACM Intl. Symposium on Mobile Ad Hoc Networking and Computing, 2002.

[7] M. T. Refaei, V. Srivastava, L. A. DaSilva, and M. Eltoweissy., "A reputation-based mechanism for isolating selfish nodes in ad hoc networks" 2nd Annual Intl. Conf. on Mobile and Ubiquitous Systems (MobiQuitous 2005), San Diego, 2005.

[8] R. Axelrod, "The Evolution of Cooperation, reprint edition ed. New York: Basic Books, 1984.

[9] 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

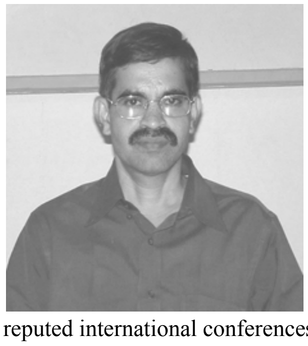
[10] Perkins C.E and Elizabeth M. Royer, "Ad hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100,1999.

[11] Haas Z. J., "A new routing protocol for the reconfigurable wireless network", Proc. IEEE 6th International Conference on Universal Personal Communications, Record: Bridging the Way to the 21st Century (ICUPC'97), pp.562–566, 1997.

[12] Park V. and Corson M., "A highly adaptive distributed routing algorithm for mobile wireless networks", Proc. of INFOCOM'97.

[13] Perkins C.E., and Bhagwat P., "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," Proc. ACM SIGCOMM'94, ACM Press, pp.234–244, 1994.

Ms Komathy K is a PhD research scholar in Anna University, Chennai. She has a vast experience in both industry and teaching. Her areas of interest are web services, wired and wireless networks and network security. She has published her research works in many reputed international conferences and international journals.



Dr Narayanasamy P is a Professor in the department of Computer Science and Engineering,Anna University, Chennai,India. His research areas are wired and wireless networks. He has produced 4 PhD candidates and one MS candidate. Presently, he has 6 PhD and 2 MS research scholars under his supervision. He has published his works in reputed international conferences and international journals.