Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in MANET

T.V.P.Sundararajan[1], Dr.A.Shanmugam[2]

[1]Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam, India

tvpszen@yahoo.co.in
Bannari Amman Institute of Technology, Sathyamangalam, India

dras@yahoo.co.in

ABSTRACT

We study routing misbehavior in MANETs (Mobile Ad Hoc Networks) in this paper. In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehaviors may exist.[1]. One such routing misbehavior is that some selfish nodes [2], will participate in the route discovery and maintenance processes but refuse to forward data packets. In this paper, we develop a game theoretic based cooperation model that observes the behavior of an intermediary node (selfish neighbors) while forwarding packets for others on a route between a source and a destination. It also allows formally study and analyze the impact of selfish behavior on the system performance.

KEYWORDS

Cooperation, selfish nodes, ad hoc network, game theory

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on pre-existing infrastructure or base stations. 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 [3],[4],[5]:

- *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.

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.

10.5121/ijnsa.2010.2212

Selfish nodes, on the other hand, which cooperate during route discovery and defect during packet forwarding, need to be explored. In this paper, we design a behavioral model that could dynamically affect the level of cooperation extended by the node towards the network functions such as routing, network monitoring and packet forwarding.

The rest of the paper is organized as follows Section 2 gives the problems caused by routing misbehavior of selfish nodes Section 3 presents proposed model defining selfish nodes. Sections 4 describe how an ad hoc network can be modeled as an infinitely repeated game. Section 5 outlines scenario study and simulation results. Section 6 discusses how to use our model to investigate the impact of different parameters as a performance evaluation. Finally we conclude our paper.

2. EXISTING PROBLEM OF SELFISH NODE BEHAVIOR

In this section, we describe the problems caused by routing misbehavior of selfish nodes.

Selfish Node Problem

One immediate effect of node misbehaviors and failures in wireless ad hoc networks is the node isolation problem due to the fact that communications between nodes are completely dependent on routing and forwarding packets. In turn, the presence of selfish node is a direct cause for node isolation and network partitioning, which further affects network survivability [6]. Traditionally, node isolation refers to the phenomenon in which nodes have no (active) neighbors; however, we will show that due to the presence of selfish node, a node can be isolated even if active neighbors are available. [7],[8]

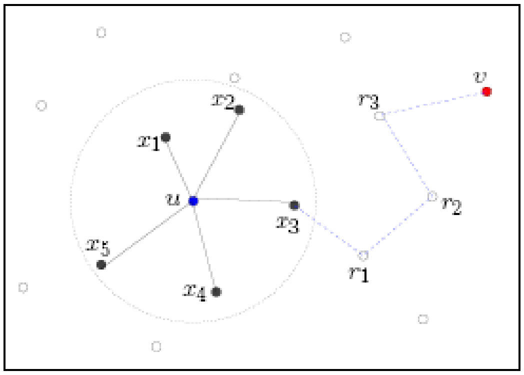


Figure.1 Node isolation due to selfish neighbors

In Figure.1, suppose node x3 is a selfish node. When node u initiates a route discovery to another node v, the selfish neighbors x3 may be reluctant to broadcast the route request from u. In this case, x3 behaves like a failed node. It is also possible for x3 to forward control packets; however, the situation could be worse since u may select x3 as the next hop and send data to it. Consequently, x3 may discard all data to be forwarded via it, and then communications between u and v cannot proceed. When all neighbors of u are selfish, u is unable to establish any communications with other nodes at a distance of more than one-hop away [9]. In this case, we say that a node is isolated by its selfish neighbors. Note that selfish nodes can still communicate with other nodes (via their cooperative neighbors), which is different from failed nodes.

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 trade off that exists between energy consumption and the network functions such as packet delivery ratio and average end-to-end delay.

3. PROPOSED MODEL

3.1. Definitions and Assumptions

We assume that time is discrete and divided in frames $t_1, \ldots, t_n$. Node i has the following information at the beginning of frame t_k:

- $Ni(t_k)$, the set of its neighbors during the frame, assumed to be fixed during each frame
- $Bi(t_k)$, the remaining energy of unit *i*,
- $\forall j \in N_i(t_k).T_i^j(t_k)$, the traffic node *i* generated as source, and that it has to send to neighbor *j* during the frame, in terms of number of packets (*j* can be the final destination for some of them and just a relay for the remaining),
- $\forall j \in N_i(t_k).F_i^j(t_{k-1})$, the number of packets, that *j* forwarded for *i* during the previous frame (*i* can be the source for some of the packets, and a relay preceding *j* in the chain for the others),
- $\forall j \in N_i(t_{k-1}).R_i^j(t_{k-1})$, the number of packets *i* received as final destination during the previous frame from neighbor *j*, that could be source for some of them and relay node for the others,
- $\forall j \in N_i(t_{k-1}).\tilde{R}_i^j(t_{k-1})$, is the number of packets *i* received from *j* as final destination, being *j* the source $(\tilde{R}_i^j(t_k) \leq R_i^j(t_k))$.

Thinking about a real mobile ad hoc network, it can be difficult to understand how the value of $F_j^i(t_x)$ is known by node *i*. If in the network communications are symmetric (i.e. $\forall i, j, k, i \in N_j(t_k) \Leftrightarrow j \in N_i(t_k)$), then for example it is possible to use a *Watchdog* unit [7], or some higher level mechanisms like end to end acknowledgements. However, it is not the main focus of this paper to explain how to compute all the needed data.

We assume that to send a packet a constant amount of energy $C\sigma$ is spent, while receiving has a negligible cost in comparison, since we assume a shared medium where a packet is received anyway from every node in the transmission range of who is transmitting. Nodes are divided in *n* energy classes $e_1, \ldots, e_n$, each with a specific generation process, without restriction.

Associated to every class e_k there is moreover a constant $0 \leq a_{ek} \leq 1$, defining the importance given to energy by nodes in e_k: if $a_{ek} = 0$ then energy is not a matter, while at the contrary $a_{ek} = 1$ implies that energy is a resource tremendously important. The class of node *i* is indicated by *e*(*i*), and it is assumed to be fixed. Finally, we are interested in modeling and understanding selfishness, so malicious behaviors are intentionally not considered. A selfish node does not want to damage any other node, it just wants to save energy while using the network.

3.2. The Forwarding Game

It is possible to model an ad-hoc network during a single frame by means of a Bayesian game [10] in the following way:

- the players are the nodes in the network,
- player *i*, as action, sets $S_i^j(t_k)$ i.e. the number of packets she will send to every node $j \in N_i(t_k)$ (a fraction of $T_i^j(t_k)$, and $F_i^j(t_k)$), i.e. the number of packets, received from j during previous frame, she will forward for her.
- the secret type of player i is her energy class *e(i)*, that affects her traffic generation distribution,
- her payoff is $\alpha_{e(i)} W_i\ (t_k) + (1 - \alpha_{e(i)}) G_i(t_k)$ ----- (1)

where $0 \leq \alpha_{e(i)} \leq 1$ is the already introduced class dependent evaluation of energy importance, $W_i\ (t_k)$ is a measure of the energy spent with success, i.e. the ratio between packets that neighbors forwarded after a request by *i*, or received as final destination, and sent packets, defined as:

$$w_i(t_k) \overset{\Delta}{=} \begin{cases} w(k) & if\ S_i(t_{k-1}) + F_i(t_{k-1}) > 0 \\ 0 & otherwise \end{cases} \qquad (2)$$

with

$$w(k) \overset{\Delta}{=} \frac{\sum_{j \in N_o(t_k)} (F_j^i(t_k) + \tilde{R}_j^i(t_k))}{S_i(t_{k-1}) + F_i(t_{k-1})}$$

and $G_i(t_k)$ is the ratio of sent packets over packets that player *i* wanted to send, defined as:

$$G_i(t_k) \overset{\Delta}{=} \begin{cases} g(t_k) & if \sum_{j \in N_{\not\subset}(t_k)} T_i^j(t_k) > 0 \\ 0 & otherwise \end{cases} \qquad (3)$$

with

$$g(t_k) \overset{\Delta}{=} \left\{ \frac{\sum_{j \in N_i(t_k)} S_i^j(t_k)}{\sum_{j \in N_i(t_k)} T_i^j(t_k)} \right.$$

- player *i* has a prior belief for every player $j \in N_i(t_k)$ i.e. a distribution on the energy class of *j*.

It is worth noting that the payoff function is always between 0 and 1, and that sending at least one packet in every frame (if there are packets to send, of course) is always at least as good as not sending anything. In a few words, every node tries to maximize its payoff function, with the following constraints:

$$c_\sigma(S_i(t_k) + F_i(t_k)) \leq B_i(t_k) \qquad (4)$$

$$T_i(t_k) \geq 0, S_i(t_k) \geq 0, F_i(t_k) \geq 0 \qquad (5)$$

$$S_i(t_k) \leq T_i(t_k) \qquad (6)$$

Constraint 4 means that it can not be spent more energy than the battery can provide and constraints 5 and 6 just better characterize the admissibility space.

A sequence of frames is the infinite repetition of the game[11],[12], with a discount factor δ depending on the mobility of the network (i.e. the probability to have a neighbor in the transmission range also in following frames): the less a neighborhood is stable, the smaller is δ, since a misbehavior by j in the present could never be punished if j is moving out of the neighborhood of i in the near future. This approach allows us to model a local knowledge, since the payoff of every player is influenced just by the moves of players modeling neighbor nodes.[13],[14].

4. MODEL DESIGN AND ANALYSIS

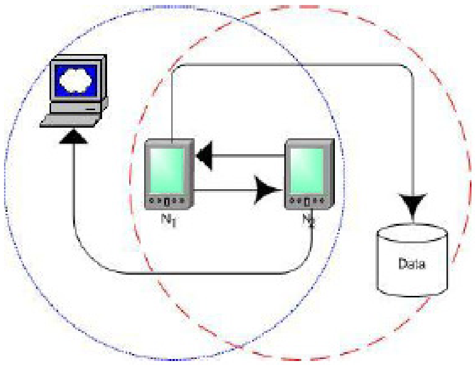


Figure 2: An Infinitely Repeat Game Model

Communications in an ad hoc network can be modeled as an infinitely repeated game. This kind of models can describe situations in which the number of rounds is finite (as it happens in a mobile ad hoc network, where nodes arrive, leave and move away changing neighborhood), but there is not the knowledge on when the game is going to stop. Every node can not be sure that it is going to play the next round with different opponents, since every node is moving.
Let us consider a “mobile” ad hoc network with two nodes that mutually need the other node to reach (for example an access point) and that also exchange messages between them (Figure 2). If there is a unique class, then there is not uncertainty about the type of the other node, and the scenario is very simple. In the single shot scenario, Nash equilibria are (of course) dependent on the value of á (and then on the energy class the nodes belong to).
If $\alpha = 0$, nodes do not care about spent energy, and their payoff function is obviously $Gi(t_k)$. For this reason, in all the equilibria of the game, nodes send all the traffic they need to (i.e. $\forall k, Si(t_k) = Ti(t_k)$, maximizing their payoff) and they forward a number of other node’s packets between 0 and the number of packets they were demanded to.
On the contrary, if á = 1 nodes are extremely concentrated on power, and their payoff is given by $Wi(t_k)$. There is just one Nash equilibrium in which nodes do not forward any packet, and send just traffic destined to the other node, since both maximize their payoff setting $Fi(t_k)$ to 0.

Finally, if 0 < α < 1, nodes are sensible to both the goals (which is a more realistic case), then a few equilibria (generally just one) exist, in which $Fi(t_k)$ = 0 for both players, and $Si(t_k)$ is the best trade off between wasted energy and throughput needs. It is possible to show that for α small enough, there exist equilibria in which more packets than the ones for the other node are sent.

If there are two different energy classes3, and $\alpha_{e(1)} \neq 0$ and $\alpha_{e(2)} \neq 0$ (i.e. both units are energy constrained), then nothing changes, since for every node the best strategy is not to forward $F_i^j(t_k) =$ 0 and to send a number of packets not much greater than the amount of packets directed to the other node $(S_i^j(t_k) \approx \tilde{R}_i^j(t_k))$, for α great enough. If $\alpha_{e(i)}$ = 0 for one of the nodes (let us suppose this holds for node 1), then it is possible to prove the following

Proposition : If node 1 belongs to class 1 with associated α_1 = 0 and node 2 belongs to class 2, with associated $1 \geq \alpha_2 > 0$, then the forwarding game in the single shot has at least $2^{S_2(t_k)}$ equilibria, in which:

• *node 1 sends all its packets, and forwards any number of node 2's packets between 0 and $S_2(t_k)$ (all the probability assignments to $F1(t_k)$ have the same payoff, leading to the lower bound on the number of equilibria,*
• *node 2 actions are conditioned by the value of α_2 and by the distribution on the type of node1.*

The first point follows directly from the definition of the payoff when α_1 = 0: *Wi(tk)* does not influence the result, which is maximized when *Gi(tk)* = 1.

Player 2, on the contrary, can raise her payoff by setting the value of *Fi(tk−1)* to 0 in every frame. After this, if α_2 is near 0, then in all the equilibria she will try to send as much packets as possible, being *G2(tk)* the important part of her satisfaction. When α_2 is closer to 1, the number and the quality of equilibria depends on her prior belief about player 1: if she thinks that the probability of having a class 1 neighbor is high, then there are more "efficient" equilibria, in which player 2 sends more packets than the one destined to player 1, trying to benefit by the power of her neighbor.

5. SCENARIO STUDY AND SIMULATION RESULTS

5.1. Scenario Study

In this part, some of the parameters are dependent on specific application scenarios, we first establish an example network scenario and incorporate the following policies in our case study and succeeding simulations.

- Every node has the same initial energy *Einit*; and may turn off packet forwarding functionality once its residual energy (normalized by *Einit*) below a threshold ξ.

- A simplified version of *nuglet counter* [15],[16] scheme is implemented to stimulating selfish nodes to be cooperative again. In this scheme, each node possesses a positive number of tokens *Iinit* initially, earns tokens when it forwards packets for other nodes, and spends tokens when it sends or receives its own packets. We assume every selfish node spends ΔI tokens in average per unit time (e.g., 1 s).

- Each cooperative or selfish node has an equal probability to be compromised by an exterior attacker, which can start to compromise a node at any (random) time. The time to compromise a node is assumed to be $\overline{Ta}$ in average. Once a node is compromised, it becomes malicious.

- The time that any node resides in the network (called residence time) is random, depending on the movement pattern of individual nodes, but with a finite expected value $\overline{Tin}$. A node is claimed to be failed once it leaves the network.

- At last, we assume an average recovery time $\overline{T}_R$ so that failed nodes can become operative again (e.g., by recharging the battery or rejoining the network).

5.2. Simulation Setup

To evaluate the correctness of our theoretical analysis, we conducted exhaustive simulations in the simulation tool *Qualnet v4.5*. The number of nodes (network size N) is ranging from 100 to 900 to represent small and large networks. The mobility model chosen is the Semi-Markov Smooth (SMS) model [20], which provides the uniform node distribution and more realistic movement patterns. Unless otherwise indicated, the speed is uniformly distributed between 0 and 10 ms to represent the movements of pedestrians and cars. Constant Bit Rate (CBR) is chosen for traffic and 100 sessions are constantly maintained, in each traffic pattern, 100 sessions are constantly maintained to keep every node involved in networking.

Moreover, in simulations nodes change their behaviors according to the energy resources available for their own use. For cooperative nodes, AODV is used as the routing protocol. While for misbehaving nodes, a modified version of AODV was developed so that their behaviors do not comply with the routing and forwarding rules defined in the standard.[17],[18] Specifically, selfish nodes do not forward RREQ and RREP messages for others; malicious nodes forward RREQ and RREP messages but drop data packets to be forwarded. The results are averaged over multiple simulation rounds conducted with various random seeds. The simulation time is set to 2000s so that the system can reach steady states. The default network parameters are listed in Table 1.

6. PERFORMANCE EVALUATION

Next, we demonstrate how to use our model to investigate the impact of different parameters, including the initial energy *Einit* and node mobility (in terms of T_{in}), on the limiting probability. In particular, the cooperative probability *Pc* is of our concern due to its importance in network survivability.[19]

6.1. Effect of Node Mobility

To evaluate the impact of node mobility on *Pc*, we conducted simulations using two different average speeds: 20 ms and 2 ms, with 10 movement patterns corresponding to each of them. The SMS mobility model used in our work provides the uniform node distribution, which eliminates the side effect of some artifacts, such as inhomogeneous node density induced by the Random-waypoint model [21] such that the effect of speed can be evaluated accurately. When the simulation area is bounded, we did not observe substantial difference in *Pc* for both average speed settings. The reason is quite simple: since all nodes are constrained within the boundary, different speeds have no effect to the node residential time, which in turn do not affect *Pi*. However, in real networks, the boundary does often not exist and nodes can hardly be confined in a given area.

Parameter	Setting
Simulation area	1000 m □ 1000 m
System size	500 (100; 900)
Transmission range	100 m
Mobility model SMS model	(uniform placement)
Movement features avg. speed	5 m=s / pause time 1 s
Link capacity	11 Mbps (1 Mbps for broadcast)
Application	CBR (64 bytes)
Traffic load	100 connections, 8 packet per sec
Simulation time	2000 s

Table 1 : The Network Setup in Simulations.

To demonstrate the impact of node mobility in real environment, we enlarged the simulation area but still assigned a 1000 m × 1000 m square as the predefined network, such that the churn due to movements can be detected. The simulation results are shown in Figure .3, in which we can see that the average speed affects Pc considerably, i.e., the higher the mobility is, and the lower *Pc* is.

To explain this phenomenon, notice the fact that the faster a node moves, the sooner the node traverses the boundary, yielding a smaller average residence timeT_{in}. Consequently, Pc is decreased due to the decreased time spent in the network. The heuristic values of Pc, annotated in the figure, are calculated by varyingT_{in}, which is simply estimated by dividing the diagonal of the network by the average speed.

6.2. The Effect of Node Cooperativeness

To observe the effect of node cooperativeness clearly, we set the recovery time as 0 so that the effect of node failures is eliminated. We also set P_B = 0 so that *Pc* varies only due to the node selfishness and Jellyfish attack. By adjusting the selfish threshold ξ and attack time *Ta*, a series of *Pc* values ranging from 0:05 to 0:95 (roughly) were obtained by using the heuristic estimation. The analytical survivability (lower bound) was then calculated for k = 1; 2; 3 with these *Pc* values. The simulation and analytic results are shown in Figure.4, where the curves with markers represent the network survivability measured from simulation data and the ones without markers are for analytical results.

From this figure, it is obvious that the network survivability increases when we decreases the connectivity requirement (k), which indicates that the stronger connectivity a network
has, the more survivable the network is in terms of its topology.

An interesting observation is that the survivability increases very fast from 0 to 1 as Pc increases, for example, the survivability for k = 2 is almost 0 as Pc ≤ 0:4; while it jumps to almost 1 as Pc ≥ 0:7. This observation is actually in accordance with the so-called phase transition phenomenon in (geometric) random graphs (see [22] and [23]) and indicates there exists a critical value of *Pc* for network survivability. Finally, we can see that the analytical results match with the simulation results with only minor deviation, and especially, the deviation becomes almost invisible when the survivability is above 0:8. This confirms the tightness of the asymptotic lower bound derived from our theoretical analysis.

6.3. The Effect of Selfish Node Misbehaviors

Impacts on Network Performance

In the similar way, we eliminated the effect of node failures in order to study the impact of node misbehaviors only. The simulation results are depicted in Figure 5. The curves in this figure also indicate that the survivability decreases when more and more misbehaving nodes are present, which is consistent with our intuition and the fact of decreased Pc. we observed that the change of survivability due to node misbehaviors is less significant than that due to node failures, especially for lower connectivity requirement. For example, the survivability for k = 1 does not decrease considerably until $Ps + Pm \leq 0.5$ and it keeps positive till $Ps + Pm \geq 0.7$. Therefore, misbehaving nodes are still active in the network layer so that they do not affect the density of active nodes μ_a, which is, however, an important factor for network survivability.

To provide a complete picture of the negative effect of node misbehaviors, we also evaluated the network performance when misbehaving nodes are present by simulations, where misbehaving nodes simply drop all data packets to be forwarded once paths are established. This is a special case of the traditional Jellyfish attack and actually called as the \Black hole" attack (different from the Black hole concept in our work). It was pointed out that the performance impact caused by this particular misbehavior is nearly the same as that caused by traditional Jellyfish attacks that manipulate the delay, reordering, and selective dropping.

Thus, we can use CBR (over UDP) to obtain a similar performance evaluation as we use TCP for traditional Jellyfish attacks . In simulations, the following metrics are considered in the evaluation: normalized throughput, average end-to-end delay, and average hop-count, with all network parameters set to the default values in Table 2. The simulation results are shown in Figure 9.

In Figure 6.(a), the normalized throughputs are shown to decrease significantly when more misbehaving nodes perform abnormal routing operations. This impact is particularly severe to the well-connected network with N = 500 nodes. The reason for the drastic degradation on throughput is partially due to the fact of substantial network partitioning effect caused by node misbehaviors, corresponding to the decreased survivability. In particular, the throughput for the network with N = 100 nodes is quite low due to the fact that the network is actually disconnected all the times.

An interesting observation is that this node misbehavior can shorten end-to-end delays significantly, especially for dense networks (e.g., N = 900), as shown in Figure 6(b). However, this plausible \improvement" is at the cost of suffocating the traffic on long paths, which is explained by the results in Figure 6(c). In fact, the decrease of average hop-count is not because shorter paths can be found; instead, it captures the effect of network partitioning and survivability downgrading.

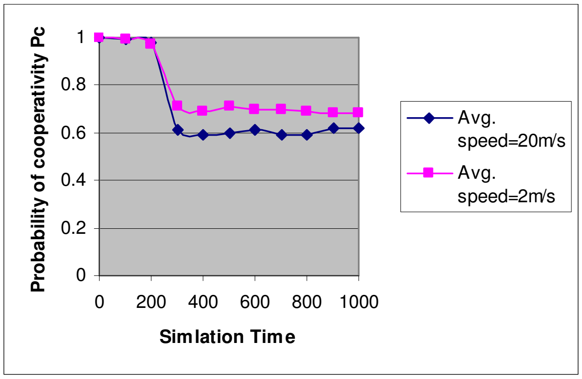


Fig 3 The Effect of Nodal Mobility on *Pc*

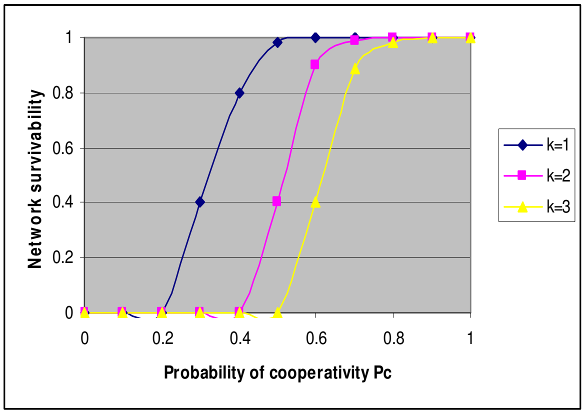


Fig. 4 Effect of Node Cooperativeness On Network Survivability

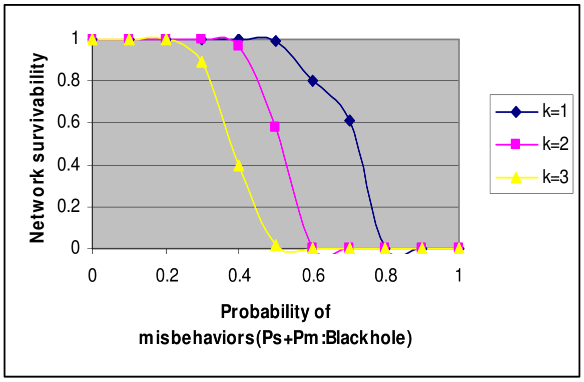
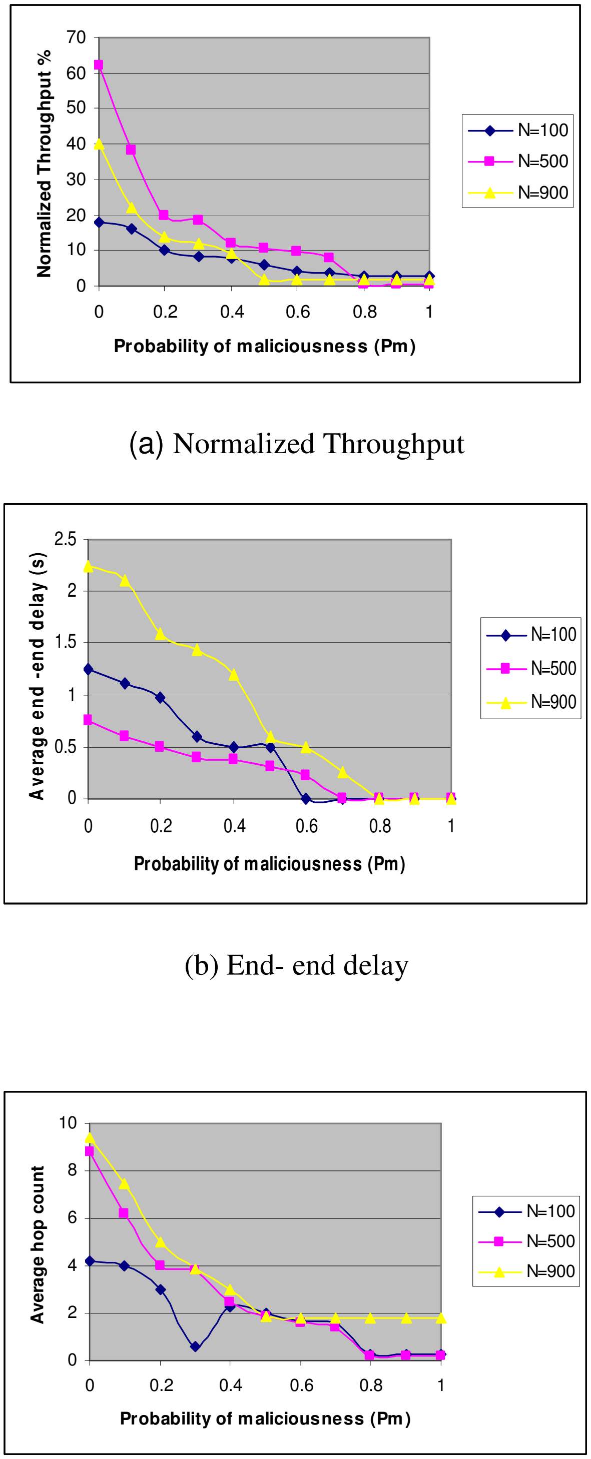


Fig.5. Effect of Selfish and Malicious Nodes on Network Survivability



(a) Normalized Throughput

(b) End- end delay

(c) Average hop count

Fig.6 Impact of misbehaving nodes on network performance

Nevertheless, although a low survivability results in a low performance, we cannot conclude a similar implication in the opposite direction. Indeed, providing a theoretical analysis on the impact of node behaviors on network performance is still an open and interesting problem, which will be our future research topic.

7. CONCLUSION

We presented a model to describe behavior of an intermediary node in a route between a source and a destination, which is a collaborative point of its one-hop neighbors. Our model is general enough to describe cooperation enforcement mechanism that have been proposed in literature in recent times, and it can be used to understand at what extent a node can be selfish, and how much can we pretend from it.

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.

Also, we study the impact of node misbehaviors and failures on network survivability, which is defined as the probabilistic k-connectivity of the network induced by active nodes. Finally, we showed that the network survivability turns out to be a function of the network properties (network size N, transmission range r, and initial density) and node behavior distributions.

As a conclusion, the impact of node behaviors (failures) on network survivability can be evaluated quantitatively from our analytical result, which can be further used as a guideline to design or deploy a survivable ad hoc network given a predefined survivability preference.

REFERENCES

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

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

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

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

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

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

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

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

[9] 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 SanDiego, 2003.

[10] 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.

[11] 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.

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

[13] S. Zhong, J. Chen, Y. R Yang, Sprite: A simple, cheatproof credit based system for mobile ad hoc networks, in: Proc. IEEE INFOCOM 2003, San Francisco, CA, United States, 2003, pp. 1987_1997.

[14] M. Stemm, R.H. Katz, Vertical handoffs in wireless overlay networks, Mobile Networks and Applications 3 (4) (1998) 335_350.

[15] M. Jakobsson, J.-P. Hubaux, L. Buttyan, A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks, in: LNCS, vol. 2742, Berlin,Heidelberg, Germany, 2004, pp. 15_33.

[16] P. Marbach, Y. Qiu, Cooperation in wireless ad hoc networks: A market based approach, IEEE/ACM Transactions on Networking (TON) 13 (6) (2005)1325_1338.

[17] L. Bla_zevic', L. Buttyán, 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 39 (6) (2001) 166_174.

[18] Y. Yoo, S. Ahn, A simple load-balancing approach in cheat-proof ad hoc networks, in: Proc. IEEE GlobeCom'04, Dallas, TX, United States, 2004, pp. 3573_3577.

[19] B. Raghavan, A.C. Snoeren, Priority forwarding in ad hoc networks with selfinterested parties, in: Proc. First Workshop on Economics of Peer-to-Peer Systems, Berkeley, CA, United States, 2003.

[20] Ming Zhao and WenyeWang. A Uni_ed Mobility Model for Analysis and Simulation of Mobile Wireless Networks. ACM-Springer Wireless Networks (WINET), September 2007.

[21] Narayanan Sadagopan, Fan Bai, Bhaskar Krishnamachari, and Ahmed Helmy.PATHS: Analysis of PATH Duration Statistics and their Impact on Reactive MANET Routing Protocols. In Proc. of ACM MobiHoc '03, Jun. 2003.

[22] B. Bollobas. Modern Graph Theory. Springer, 1998.

[23] Mathew Penrose. Random Geometric Graphs. Oxford University Press, 2003.

Authors

T.V.P. Sundararajan received the BE Degree in Electronics and Communication from Kongu Engineering College , Perundurai in 1993 and the ME Degree in Applied Electronics from the Government college of technology, coimbatore in 1999. He is Assistant Professor ,working in Bannari Amman Institute of Technology, Sathyamangalam. He is doing a part time research in Anna University, Chennai . His current research focuses on mobile ad hoc networks and wireless security. He is member of the IEEE, ISTE and the IEEE computer society.

E-mail : tvpszen@yahoo.co.in

Dr.A.Shanmugam received the BE Degree in PSG College of Technology in 1972, Coimbatore and ME Degree from College of Engineering, Guindy, Chennai in 1978 and Doctor of Philosophy in Electrical Engineering from Bharathiyar University, Coimbatore in 1994.From 1972–76, he worked as Testing Engineer in Testing and Development Centre, Chennai. He was working as a Lecturer Annamalai University in 1978. He was the Professor and Head of Electronics and Communication Engineering Department at PSG College of Technology, Coimbatore during 1999 to2004. Authored a book titled "Computer Communication Networks" which is published by ISTE, New Delhi, 2000.He is currently the Principal, Bannari Amman Institute of Technology, Sathyamangalam. .He is on the editorial board of International Journal Artificial Intelligence in Engineering & Technology (ICAIET), University of Malaysia, International Journal on "Systemics, Cybernetics and Informatics (IJSCI)" Pentagram Research Centre, Hyderabad, India. He is member of the IEEE, the IEEE computer society.

E-mail : dras @ yahoo.co.in