Assessing Trustworthiness of Nodes to Enhance Performance in Mobile Ad hoc Networks

Sanat Kumar Bista, Keshav Dahal, Peter Cowling
AI Research Group
University of Bradford
Bradford BD7 1DP, United Kingdom
{s.k.bista, k.p.dahal, p.i.cowling}@bradford.ac.uk

Aziz Bouras
IUT Lumière
Université Lumière Lyon 2
Lyon, France
abdelaziz.bouras@univ-lyon2.fr

Abstract—This paper presents an application of reputation based trust assessment model in mobile ad hoc network setting. A game between the Sender (originator) and Intermediary (forwarder) nodes in the network is modelled and plugged-in to a trust assessment framework that classifies feedback according to past acquaintances between the nodes. Simulations for the experiments have been carried out in an Iterated Prisoner’s dilemma like setting, where each player represents a network node. Through our experiments we show that having trust model decreases the Packet Drop Ratio (PDR) in an ad hoc network setting. Further, the results show that Gain through the utility and savings of energy is better with application of the trust model.

Keywords-Mobile ad Hoc Networks; Reputation; Trust; Trust Models

I. INTRODUCTION

Mobile Ad hoc networks also known as MANETs are complex, distributed, dynamic, self-organizing wireless mobile nodes which can form arbitrary networks in a situation with no pre-existing communication infrastructure [1]. Increasing popularity of light-weight devices such as handhelds, PDAs, cell phones, laptops etc are facilitating the ubiquitous computing vision of service access anytime, anywhere [2]. Applications of such networks can be seen in Collaborative Computing, Mesh Networks, Wireless Community Networks etc to name a few. In such scenario, while forming temporary networks, the devices might need to pair up with known or completely stranger ones –being unaware of the quality of service that might evolve from the collaboration. As the nodes in mobile ad hoc networks are routers as well as terminals, it is on the nodes themselves to assess whether collaboration with some particular node is desirable or not. As a part of collaboration, cooperation means finding a path for packet and forwarding it to others [3]. These networks are further characterized by a constrained bandwidth, processing and storage power and battery life [4]. This gives a dilemma on whether to be cooperative by forwarding the packets or conserve ones recourses and defect sender by dropping the packets. There is also a serious security concern in such networks. The nodes here have inadequate protection against malicious attacks which could lead to hijack of the forwarding nodes by misbehaving and malicious sources [5]. As nodes tend to be strategic, deflection could either be due to a merely faulty node, a node’s selfishness to conserve its energy, or an act of a strategic node trying to maximize its gain from the action. It becomes thus necessary to identify a trustworthy node for collaboration. Classical security mechanisms are inept in solving problems which are due to the node’s selfishness or inactivity [6].

Trust and Reputation management issues are critical in networks with nodes performing services on behalf of other nodes, examples of this include P2P, Grid, and wireless ad hoc networks [7]. In ad hoc networks the behavior of individual nodes has profound impact on the overall network performance – due to the fact that there is no centralized control [8]. The idea of trustworthiness assessment based on reputation information is widely practiced method of assuring service quality in e-commerce, Peer to Peer and multi-agent environments [9-13]. Feedback scores of buyers and sellers in eBay pages [14], is an example of trustworthiness assessment in online marketplace setting. Problem of trustworthiness assessment in Mobile Ad Hoc Networks (MANETs) have also been explored by several literature, e.g. [3, 15-17].

Our investigation in this paper concerns modeling interaction between nodes in ad hoc networks as games. We then study usefulness of a reputation based trust model in such scenario. Particularly, we study the effectiveness of trust system in controlling malicious behavior of nodes and conservation of node’s energy. We use an acquaintance based trustworthiness assessment framework that we developed in [18] to simulate our game models. The usefulness of weighing feedbacks according to past acquaintances in situations with need to prioritize feedbacks (example taken is Online business environments) is explained well through results in [18]. We see that significance of an acquaintance based aggregation method is high in mobile ad hoc settings as well. In general, mobile ad hoc networks are perceived as dynamic, temporary and strategic network, but, certain flavors of it can also permit
repeated interactions within a fixed group. Examples of such settings can be class room networks, which though temporary, might have repeated interactions. Other example can be a network of frequent, loyal customers of a Coffee Shop enjoying networking with other visitors. The later example also includes repeated interactions. Thus, in settings like this, it becomes sensible to weigh the reputation of individual nodes based on the nature of past association.

The remaining part of this paper is arranged as follows: section II presents an overview of related works, experimental model is explained section III, settings for experiments and results are presented in section IV. Finally section V presents conclusion and possible future work in this area.

II. RELATED WORK

We present a review of some approaches based on reputation techniques that have shown to have positive impact on improving cooperation and assessing peer trustworthiness in MANETs. Buchegger and Boudec in [3] describe the use of a reputation based self policing mechanism to immunize ad-hoc networks from the presence of misbehaving nodes. Misbehaving nodes in the network are identified through reputation systems and second hand information using the deviation test. The actual test of deviation done here is between second hand information and the node’s reputation value. Once identified, such nodes are automatically isolated from the network. In an earlier work by the same authors reported in [15] they have proposed a protocol called CONFIDANT based on selective altruism and utilitarianism that would make misbehavior unattractive among the nodes. Routing and forwarding behavior have been taken as ingredients of this model. An analysis of CONFIDANT was later done by Mundinger and Boudec in [17]. The authors have analyzed the robustness of the system against liars in the network. Using a mean field approach to a stochastic process model, they have shown that liars have no impact until the number exceeds certain threshold. However, we think that, besides the reputation information, analysis of the behavior of nodes is also necessary to complement an assessment model.

Another model of reputation based technique to enforce collaboration is suggested by [16]. This technique uses a weight based approach to compute reputation by aggregating Subjective Reputation, Indirect Reputation and Functional Reputation. The computed reputation value is used to make decision on collaboration. The method however takes account of the positive reputation information only. The authors say that negative ratings aren’t communicated between nodes, as this information could be hacked by malicious nodes to decrease reputation of other nodes. We see that negative ratings have quite significant value in reputation systems, specifically in identifying the cooperation probability of a particular node. Strategic nodes can always manipulate positive ratings as well. We are of the opinion that negative ratings should also be equally used in identifying trustworthy collaborators.

In [19] the authors have presented Semi-ring based trust evaluation metrics, which views the trust inference problem as a generalized shortest path problem on a weighted directed graph. The nodes of the graph represent entities and the edges represent trust relations. The major contribution of this paper is in proposing a method establishing trust among two nodes which had no previous direct interaction records. In [20] the authors have proposed a Secure and Objective Reputation based incentive scheme(SORI) that claims to encourage packet forwarding and discipline selfish behavior. Selfish nodes in this scheme are penalized by a punishment scheme which relies on probabilistically dropping packets originating from such nodes.

Our work extends the literature by analyzing the usefulness of an acquaintance based trust model in promoting cooperation among the sender and intermediary nodes in a network.

III. EXPERIMENTAL MODEL

The game conceptualized here is in between two parties, namely the Sender Node (S) and the Intermediary Node (I). In this game we do not consider the target node as it has no influence in packet transmission. A sender node is the one that initiates the transmission of the packets, which the intermediary nodes will have to relay to the final destination node. As a characteristics of nodes in an ad hoc network, each node being powered by battery, has a limited amount of energy available to process its own data in addition to that of forwarding packets for others. Thus, there lies a tendency among the nodes to conserve energy through a Deceptive act of dropping packets from the sender nodes. The presence of malicious nodes makes the situation further complex. A malicious sender node originates packets which have ill motive of draining energy resources of peers in the network. In this scenario, the two possible moves and their meanings for each type of node are:

a. Sender Node (S): For a sender node, a cooperating act (C) means forwarding a genuine packet for transmission. Defection (D) means sending malicious packet to intermediary nodes for transmission.

b. Intermediary Node (I): For an intermediary node, a cooperating act (C) means forwarding the packets from the sender node to the designated final node or an intermediary node en-route. A deceptive act (D) in this case means dropping the packets (not forwarding).
Let $\epsilon$ represent the unit of energy consumed by each transmission and $G$ be the gain associated with any transmission. For simplicity reasons, we assume that gain $G$ of a transaction can be expressed as a numerical value. In business game settings, cost price of goods can be related to a gain like that mentioned above [21]. From a game theoretic perspective, gains can be numerically represented by the average payoff obtained through each interaction. Further, we assume that the gain obtained through defection is $x$ times the gain that would have been obtained through cooperation. Here, $x$ is an integer and is greater than or equal to 1 ($x \geq 1$). Also for the purpose of our model, we consider energy to have certain numerical representation which is compatible with the gain value. The four different possible outcomes (in terms of payoff) of the game between a sender node and intermediary node are explained below:

**CASE I: Sender Cooperates, Intermediary also cooperates**

In this situation, the sender node forwards a genuine packet and the Intermediary node forwards the packet to next level. Both of the nodes receive a reward payoff. We quantify this as the total gain $G$ minus the energy consumed for the transmission. Thus,

- **Reward Sender**, $R_S \rightarrow (G - \epsilon)$  \hspace{1cm} (1)
- **Reward Intermediary**, $R_I \rightarrow (G - \epsilon)$  \hspace{1cm} (2)

**CASE II: Sender Cooperates, Intermediary Defects**

The sender node in this case sends a genuine packet for transmission, but the Intermediary node drops it. The sender node here receives a *Sucker’s Payoff* which is quantified in terms of loss of the expected gain and energy. The defecting intermediary receives a *Temptation Payoff*, which is equal to savings in energy plus the multiplied gain. Thus,

- **Sucker’s Sender**, $S_S \rightarrow -(G + \epsilon)$  \hspace{1cm} (3)
- **Temptation Intermediary**, $T_I \rightarrow ((x \times G) + \epsilon)$  \hspace{1cm} (4)

**CASE III: Sender Defects, Intermediary Cooperates**

In this case, the sender node defects by forwarding a malicious packet to the intermediary, while the intermediary forwards the packet further on. The sender receives a *Temptation Payoff* equivalent to the multiplied gain (less the energy spent), while the intermediary receives a *Sucker’s Payoff* equivalent to loss in energy and gain.

- **Temptation Sender**, $T_S \rightarrow ((x \times G) - \epsilon)$  \hspace{1cm} (5)
- **Sucker’s Intermediary**, $S_I \rightarrow -(G + \epsilon)$  \hspace{1cm} (6)

**CASE IV: Sender Defects, Intermediary also Defects**

The sender node in this case defects by forwarding a malicious packet, and the intermediary node also defects by dropping the packet. Both in this case receive a *Punishment Payoff*. As the packet was dropped, sender could not gain anything out of the malicious transmission, thus its payoff can be represented by the loss in the amount of transmission energy. For the intermediary, it conserved its energy, but it lost the expected gain out of the transmission. Thus,

- **Punishment Sender**, $P_S \rightarrow -\epsilon$  \hspace{1cm} (7)
- **Punishment Intermediary**, $P_I \rightarrow -G$  \hspace{1cm} (8)

This can also be summarized in the pay-off matrix as given in Table I:

<table>
<thead>
<tr>
<th>Sender Node (S)</th>
<th>Cooperate (C)</th>
<th>Defect (D)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$R_S \rightarrow (G - \epsilon)$</td>
<td>$S_S \rightarrow -(G + \epsilon)$</td>
</tr>
<tr>
<td></td>
<td>$R_I \rightarrow (G - \epsilon)$</td>
<td>$T_I \rightarrow ((x \times G) + \epsilon)$</td>
</tr>
<tr>
<td><strong>Defect (D)</strong></td>
<td>$T_S \rightarrow ((x \times G) - \epsilon)$</td>
<td>$P_S \rightarrow -\epsilon$</td>
</tr>
<tr>
<td></td>
<td>$S_I \rightarrow -(G + \epsilon)$</td>
<td>$P_I \rightarrow -G$</td>
</tr>
</tbody>
</table>

There lies a dilemma in this game on whether to be cooperative by forwarding the packets or conserve ones resources and defect sender by dropping the packets. We relate this dilemma to that in iterated prisoner’s dilemma game [22-24], which says that the following inequalities between the payoffs (Temptation: $T$, Reward: $R$, Punishment: $P$ and Sucker’s: $S$) must hold true in order for the dilemma to exist:

\[
T > R > P > S
\]

and

\[
R > \frac{T+S}{2}
\]
Based on this, we have the following payoff inequalities for the sender and the intermediary nodes imposed throughout the experiments. The numerical values for these parameters during the experiments were chosen such that it honors the fundamental requirements for the dilemma to exist. Thus, in this case the pay-off models are:

**a. For Sender Node**

\[(x * G) - \epsilon > (G - \epsilon) > -\epsilon >- (G + \epsilon)\]  

(9)

and,

\[(G - \epsilon) > \\frac{(x * G) - \epsilon + (G + \epsilon)}{2}\]  

(10)

**b. For the Intermediary Node**

\[(x * G) + \epsilon > (G - \epsilon) > -G > - (G + \epsilon)\]  

(11)

and,

\[(G - \epsilon) > \\frac{(x * G) + \epsilon + (G + \epsilon)}{2}\]  

(12)

We use this payoff model to simulate our experiments.

### IV. EXPERIMENTAL SETTING AND RESULTS

Our experiment here concerns the application of the acquaintance based trustworthiness assessment model we developed in [18] to the mobile ad hoc game described in section III. We investigate the effectiveness of the trust model by analyzing two factors in particular: i. the packet drops in the network, ii. trend in the Gain of the nodes. Adapting [18] to our situation, reputation of a node in the game is based on the number of cooperative or defective actions (forwarding or dropping of packets) in the past, but we have further made a careful distribution of weights across the reputation of nodes classified according to their acquaintance with the subject node (the node assessing trustworthiness). Three different categories of nodes can be labeled accordingly:

**Most Direct Node** (m) is the player itself. Most direct Node reports its own experiences of the past interactions.

**Gray Nodes** (g) represents the nodes with which both of the nodes considering a transaction have interacted in the past.

**Opposition Friendly Node** (o) is the node which has only interacted with the opposition (the other party of sender or receiver) and not the self in the past.

Probability of cooperation from each node is calculated by using the transaction history containing the number of Cooperation and Defects. This is produced by calculating the expected probability of cooperation of a beta distribution for any node \( p_n \) as given in equation (13):

\[E(p_n) = \frac{C_n}{(C_n + D_n)}\]  

(13)

Where \( C_n \) represents the total number cooperative actions of node n and \( D_n \) its total number of defective actions in the past.

If \( m, g, \) and \( o \) represent the past record of Most Direct, Gray and Opposition Friendly nodes respectively, then the Trustworthiness Factor (TwF) of node \( Y \) as assessed by node \( X \), based on the probability expectation of Beta Distribution is given by:

\[\text{TwF} (n_{XY}) = \text{W}_{MR} \sum \text{E(P)}m + \text{W}_{GR} \sum \text{E(P)}g + \text{W}_{OR} \sum \text{E(P)}o\]  

(14)

Where \( \text{W}_{MR} \), \( \text{W}_{GR} \), and \( \text{W}_{OR} \) are the weights associated with each report and \( \text{W}_{MR} + \text{W}_{GR} + \text{W}_{OR} = 1 \). The variables, \( i \) and \( j \) represent the total number of gray nodes and opposition friendly nodes respectively. The value for \( \text{W}_{MR} \), \( \text{W}_{GR} \), and \( \text{W}_{OR} \) are obtained from the evolutionary data, as the game continues. The Most Direct Report (MR) being a direct representation of first hand information (zero hop reporters) is considered to be more influential in decision making and thus is assigned to as \( \text{W}_{MR} \). Out of the remaining sum available for weight (this is dynamic over the game), three quarters is assigned to \( \text{W}_{GR} \) and one fourth is assigned to \( \text{W}_{OR} \). This approach gives a least priority to the report from the players with whom no game has ever been played, but at the same time does not ignore them totally.

The experiments for this investigation were carried out in an Iterated Prisoner’s Dilemma like setting over a spatial distribution of players. A memory-3 game with four specific possible moves (CC, CD, DC, DD) is played between the nodes thus making the chromosome size 64 (4³). In this game, an action on what to do next will be guided by the particular strategy that matches the past three histories of interactions that each node maintains.
Our choice of 3-memory has to do with strategy representation. We need the representation to be comprehensive such that it is capable of representing a wider range of strategies. Axelrod in [23] used additional 6 bits to determine the first three moves. A variation of this was used by Errity in [25] and we are following the same scheme of additional bit encoding, in which 7 extra bits are used for encoding actions for the first three relative moves (relative to opponent moves). In this approach it is not required to encode an assumption of the pre-game history [25]. For reproduction, the system is capable of performing a crossover as well as mutation. One-point crossover [26] is used to break the parent chromosomes at the same random point. The payoff values as obtained would work as a fitness function for the GA based simulation. The system here, searches for an optimal strategy.

Nodes in MANETs vary in numbers depending on the type of network they form and whether they are also connected to the Internet via some networks. For the purpose of our experiments we select parameters by first considering an ad-hoc network of 25 nodes, where each node would act alternately as a sender and forwarder. At a particular time, the sender-forwarder pair would play the forwarding-dropping game as explained in section III. We conducted the experiment with various settings for the number of iterations for the game (number of packet exchanges to be made before calculating a strategies’ fitness), and the length of the evolution. Our simulation result-over 5 rounds- showed that for 25 nodes, with 10 packet exchanges in each generation, an evolution length of 50 generations would show stability in the average gain of the nodes. Thus, we choose an iteration value of 10 and evolution length of 50 generations for the whole experiment (with 25 nodes). Crossover probability and mutation probability were kept fixed at 0.98 and 0.01 respectively.

For the experiment, we assume a numerical value of 5 for the maximum gain (G) and a value of 2 for the multiplier factor $x$. These values have been chosen such that the condition for dilemma are not broken. Further, we assume that each transmission of packet (whether malicious or genuine) will consume unit energy. With these values, we see that the inequalities in equation 9, 10, 11 and 12 are fulfilled, meaning that there exists a dilemma on whether to cooperate or defect.

We conducted the simulations, the results of which are presented and explained in the sub-sections below.

A. Result I: Packet Drop Ratio
The first thing we analyzed in experiment was impact of our reputation model in the Packet Drop Ratio. A Packet Drop Ratio is the ratio of total packets dropped by a node to that of forwarded ones. Thus, the lower the ratio, the better is the cooperativeness of the nodes.

We first carried out the simulation in a setting where there was no presence of a reputation model at all. Followed by this was a game with a small reputation threshold of 0.2, progressing further to an expected trust worthiness of 0.5, and 0.9. Threshold ($T_H$) determines the minimum level of trustworthiness expected from the opponent in order to play a game. The opponents trustworthiness calculated by the trust model is a real number whose value lies between 0 and 1 (inclusive), and is comparable to the threshold. The trustworthiness here is calculated using equation (14).

The packet drop ratio for the 25 nodes obtained after an evolution is given in figure 1.

![Figure 1 Packet Drop Ratio for the nodes in network (with the first bar from bottom for PDR-No Reputation, second for PDR TH=0.2, third PDR=0.5 and fourth PDR=0.9)](image-url)
The result trend here shows that the packet drop ratio for the nodes was high with no reputation system at all, and that they lowered with the increase in the expected cooperation from the opponents. Figure 2 shows average of this ratio at various thresholds.

![Figure 2 Average Packet Drop ratio at various thresholds.](image)

An average packet drop ratio of 1.39 was seen when there was no reputation system. This lowered down to 0.80 with threshold of 0.2, to 0.28 at threshold 0.5 and 0.09 at threshold 0.9. This trend shows that, an ad hoc network setting without a reputation based assessment model is very vulnerable to packet drops and malicious packet forwarding. With our reputation system in place the tendency to drop packets and forward malicious packets were reduced significantly. This has shown the effectiveness of our model.

B. Result II: Average Gain

The other thing we have analyzed through our experiments is the average gain obtained through each transmission throughout the evolution length of 50 generations. The two factors that contribute to gain (G) in our ad hoc game model are the energy factor and the multiplier factor. The energy factor contributes to gain by conserving each node’s energy (by dropping packets), and the multiplier factor increases the gain by obtaining payoff for deceptive behavior. Figure 3 shows that evolution trend of the average gain.

![Figure 3 Evolution of Average Gain in different thresholds.](image)

The result seen in the graph is in line with the average packet drop ratio in a sense that, in each category, with decreasing packet drops, the average gain has increased. This shows that the reputation model applied to the network setting has played a constructive role in optimizing the transaction gain and energy savings. The fact that the average gain did not cross the maximum gain value of 5 that we had chosen for the experiments show that our model has discouraged the contribution of defection due to multiplier effect in payoff.

Both of the results above have shown that our model has been effective in curbing temptation of nodes to defect each other. This shows usefulness of a trust model in mobile ad hoc network settings.

V. CONCLUSION AND FUTURE WORKS

This paper discussed an application of trust model in the mobile ad hoc network setting. The usefulness of the model was demonstrated by the system’s capability to enhance cooperation between the nodes by decreasing the packet drop ratio and optimizing the gain. The results support the fact that assessing trustworthiness filters defaulters from coming into action while at the same time promotes cooperation and conserves node energy. Possible future work in this area is to extend the sender-intermediary game...
by considering receiver nodes also in the game. This necessarily means that the game in such scenario would be n-player. Such model is believed to be more realistic, as it does not constrain the role of receiving node in the quality assurance procedure.

ACKNOWLEDGMENT

This research has been supported by the EU Asia-link project - TH/Asia Link/004(91712) - Euro-Asia Collaboration and Networking in Information Engineering System Technology (EAST-WEST). Many thanks to three unknown reviewers of the paper for an in-depth review.


