Managing Reputation over MANETs

G. Bella, G. Costantino, S. Riccobene
Dipartimento di Matematica e Informatica, Università di Catania
Viale A.Doria, 6 — I-95125 Catania, ITALY
{giamp,costantino,sriccobene}@dmi.unict.it

Abstract

The use of small portables and mobile devices has made MANETs (Mobile Ad Hoc Networks) very popular. A MANET is a network composed by a group of mobile nodes without any fixed device or a central coordination. They work in an open net and their collaboration is the sole means to allow communications and the survival of the MANET itself.

A critical issue is to assess the behaviour of the nodes that participate in the network, possibly identifying selfish conduct that can compromise the functioning of the system. This paper shows a method to evaluate the behaviour of all nodes by establishing a reputation value that represents the trustworthiness of each node.

A protocol is presented to calculate the reputation of a node by locally observing the node from another one, and then tuning this intermediate value with additional observations from other participants. When the reputation value of a node is available, it is circulated and distributed uniformly over the network.

This reputation protocol is viable. Each node can efficiently calculate the reputation values of its neighbours and then of all network nodes. A variety of simulations conducted using the network simulator NS-2 strongly support these claims.

Keywords: MANETs, Reputation, BUG, Cooperation, NS2.

1 Introduction

With the proliferation of mobile lightweight terminals, like smartphones or PDAs, the need for communication using wireless short/middle-range channels is grown. A Mobile Ad Hoc Network (MANET) is a structure composed only by wireless nodes, without any fixed devices, like routers or hubs. This kind of network is set up instantly, as soon as devices, which do not even know each other, are available. It survives until the participants remain linked together.

The main feature of a MANET is the collaboration between its participants, "nodes" in the following. Collaboration is necessary to allow multi-step communication. In fact, the physical layer of a wireless system imposes strict bounds to a direct connection, so that pairs of nodes that are too far apart can exchange packets only through the cooperation of other intermediate nodes. The packets flow through the network via hop-by-hop routing. This clearly requires that a transit node uses its own energy to provide the connectivity used by other nodes. The transit node does not receive any direct advantage in such a collaboration: if it does not forward packets, it saves its energy, but the network falls down. Because energy, in mobile devices, is often provided by a small battery, nodes are attracted to assume a selfish behaviour, using energy only for personal convenience.

In such a scenario, it is important to focus our attention on the conduct of the nodes, analysing their behaviour in order to define policies that encourage collaboration. A way to summarize the behaviour of a node is to establish its reputation, observing its involvement in other communications. The literature features various definitions of reputation. For example, in [8] J. Liu and V. Issarny say that the reputation toward an agent can be seen as a prediction on that agent's future actions. In our work the concept of "node reputation" is essentially a measure of the collaboration provided to maintain the network connectivity, forwarding messages of other senders.

With this definition, the value of the reputation can be used as a starting point to generally incentive collaboration, or to define a power-save routing protocol. Quite simply, if a node with a low reputation wants to initiate a communication, its request obtains a low priority and therefore low resources.

An evaluation of the neighbour reputation can be quite simple using direct observation. The main problem in using reputation in a distributed environment without central coordination such as a MANET is the circulation of the reputation information over the network. A network node

978-0-7695-3324-7/08 $25.00 © 2008 IEEE
DOI 10.1109/IAS.2008.24

must have values respectively indicating the node's perceived reputation of each another node. A viable reputation protocol should keep the reputation values of all nodes about a specific node as similar as possible.

A node can take a selfish behaviour in a position, and then move into another region of the network taking a collaborative one. The circulation of its reputation towards all network nodes can disincentive such a double-face conduct.

Generally speaking, in a distributed environment an agent (a node for us) can take one out of three different behaviours, according to the BUG threat model [1]. By recasting that model when the goal is reputation, if follows that each node can be:

- good: when it uses its resources, as energy, to provide services to other nodes without any direct interest;
- bad: when it is essentially selfish, and damages the network intentionally by neglecting or limiting particular communications.
- ugly: when it essentially assumes a good or bad behavior according to its cost/benefit analysis of the context.

It is clear that only when acting as good, does a node provide support to the network, forwarding packets of other nodes. When a node takes a bad role, it can cause loss of data and the network can be split, isolating a number of nodes. This type of behaviour strongly depends on the context where ugly nodes operate, as they may decide to collaborate or not.

We do not consider the problem of associating an identity to a node. In this work every node maintains its unique identity everywhere. This assumption can be brought to hold in practice using for example the DAA protocol (Direct Anonymous Attestation) [3]. That protocol is based on the use of a TPM [5], which allows a certain level of anonymity.

We present a protocol to handle reputation using information obtained with a multi-step knowledge process (neighbours' neighbours observation). We also developed an NS2 [11] simulator that implements all features of the proposed solution. Modifying NS2 agent that use the IEEE 802.11 protocol and the Dynamic Source Routing (DSR) [6]. It was pleasing to obtain evidence that the reputation values are efficiently computed and distributed over the network.

The rest of the paper is organized as follows. In the following section we discuss about related work regarding reputation in mobile networks. Then, we introduce the problem of good and selfish nodes in an Ad-Hoc network, defining our solution to evaluate the reputation of all known nodes. After that, our simulator and the obtained results are presented. Finally, we conclude the paper with some guidelines for future research.

2 Related Work

The meaning of reputation and trusting in the literature has changed repeatedly and there is no a global consensus [7]. It depends on the context in which is used. March [9] was the first to advance a formal concept of trusting and a model that does not include reputation.

Liu and V. Issarny in [8] noticed that "*trust towards an agent can been seen as a prediction on that node's future action*" and that "*an important factor affecting the prediction is the reputation of the agent*". They define a model based on the quality of the service that the node provides, but do not consider selfish behaviours.

In [2] Bistarelli and Santini give a definition of reputation "*based on recommendations received also from other nodes*" advancing the concept of multitrust. The trust that a node puts in another node will vary when the latter collaborates with other nodes.

S. Buchegger and J. Le Boudec in [4] introduce a model to help the isolation of misbehaving nodes and to avoid that good nodes do not collaborate with malicious ones.

To enforce collaboration, Michiardi and Molva [10] suggest a protocol to prevent and to individuate selfish nodes. The method CORE calculates the reputation of all nodes and detects selfish behaviour. It also helps the nodes to share such information.

None of these contributions is directly related to ours. In fact, our main aim is to establish a node's reputation value about any other participating node, and to use this information for subsequent power-saving routing protocols. For example, even the information circulated according to Michiardi and Molva [10] does not reach a stable reputation value that all nodes perceive about a given node. Without such value, it is impossible to implement network power-saving routing.

3 The Proposed Protocol

In order to assess reputation, we introduce a protocol to evaluate the behaviour that a node keeps. The protocol initially relies on the local perception of a node, and then refines it by the recommendations provided by other nodes.

3.1 Reputation by Direct Observation

The basic idea of our protocol is that a node reputation grows only if it forwards packets of another sender, calling "sender" the node which the communication starts from. The node under analysis has no interest in that connection: on the contrary, it uses its energy only to forward others packets.

Let us consider a simple scenario: a node with only two neighbours (node B in figure 1) into the route of a multistep

communication (A->C). It forwards packets received from node A to node C (because communications are often bidirectional, the roles of A and C are inverted in the response phase).

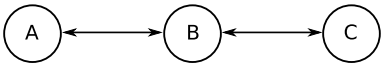

Figure 1. A simple model

Node A can compute Bs reputation observing the packets it receives from B. A cannot perform a direct measure of the packet it sends to B that must be forwarded to C; it can obtain an indirect response of this step observing the return traffic, which is composed by packets that B forwards to A. With this method, a unidirectional traffic in a multistep communication, involves a growth in the reputation of the j-th node known by the (j-1)-th. Clearly, a bidirectional traffic provides more information. It is obvious that a node considers its incoming traffic for reputation computation only if the origin is at least two steps far. This means that a node discards, for reputation purposes, any traffic starting from its direct neighbours because these have direct interest in those communications. So this traffic is normally forwarded, but it does not contribute to the reputation measurement.

The information acquired by direct observation are stored in a table, called *Neighbour Reputation Table* (NRT), which keeps track of the data amount received from closest nodes. Due to the fact that packets in a bidirectional communication can be constituted also by a simple ack, the values stored in the NRT must consider the number of packets received and their size.

The following figure shows an example NRT:

Node	Forwarded		Generated		R_{loc}
B	47	10	60	20	0,41
E	15	8	20	5	0,70

Table 1. NRT of a generic node

Starting from this information, we derive the *Local Reputation* using the following definition:

$$R^i_{loc}(j) = \frac{aP^i_f(j) + bD^i_f(j)}{aP^i_g(j) + bD^i_g(j)} \quad (1)$$

where $P^i_x(j)$ represents the packets that node j sent towards node i and $D^i_x(j)$ represents the amount of data that they carry. The sub-index g identifies data that are generated by node j; instead, sub-index f identifies data that node j forwards (i.e. the source is different from j). See figure 2.

The parameters a and b let us give different weights to number of packets and amount of data received.

The formula expresses the local reputation of node i about node j. It shows the ratio of the amount of information forwarded by j and the amount of information that it generated. From the point of view of node i this ratio represents the degree of unselfishness in the use of the link j-i. The higher the amount of traffic that j generates, the lower its reputation. On the contrary, the higher the amount of data forwarded by j, the higher its reputation.

In other words, this definition of local reputation is a measure on the percentage of the energy that j used for its own purposes with respect to the energy that it used to forward traffic of other nodes, in which j has no interest.

We must point out that this definition for the reputation implies a bounded view of the node under observation; clearly, every neighbour of that node could calculate a different value for its reputation. So, it is necessary to introduce a protocol to mix these values, to obtain a uniform one. Also, it is necessary to scatter this information towards far nodes, that are not directly connected to it. This issue is addressed below.

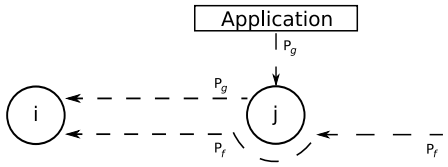

Figure 2. Different packet handling

3.2 The Global Reputation Table

The NRT contains only information on one-hop-far nodes. Every node maintains also the so called *Global Reputation Table* (GRT), that stores information about all nodes in the network.

The aim of this section is to present a methodology to maintain the values stored in these tables almost uniform all over the network, so that they can be used to implement policies that avoid (or limit) selfish behaviour.

The structure of the GRT is very simple: it contains an entry for every known node, to store its reputation. There are two different ways to determine these values:

- if the node is not a neighbour, the value is calculated from the information scattered by other nodes;
- if the node is directly connected (and can be observed), the value is calculated using the personal NRT and remote information. This procedure assures that local reputation is tuned using remote observation.

The exact expressions to be used will be presented in the following.

3.3 Reputation Table Exchange

As described above, every node of the network constructs an NRT, tracing one-hop-neighbours nodes, and a GRT, for neighbours and far nodes. Periodically, the information in the GRT are shared with the others, exchanging such tables. This protocol allows to scatter the value of a reputation throughout the net, in order to populate the GRTs with information on all participants to the MANET.

According to [8], we call *Recommendation* about x from y the local reputation seen by y regarding x. So, we will indicate with Recommendation every information acquired from the GRTs of the neighbours.

Table information is not broadcasted all over the net with a flooding procedure, but precisely. Every node that receives a table from one neighbour, calculates new values, and then, with a prefixed schedule, it sends the new GRT to its neighbours.

This kind of sharing limits the traffic in the net, avoiding the overload and limiting the use of energy. However, it can involve a non-uniform distribution of the same value. This issued can be addressed by choosing the correct time interval between sending the GRT, and launching the reputation update procedure described below.

3.4 How to Estimate the Global Reputation

Expression 1 introduced the local reputation $R^i_{loc}(j)$ estimated by a node i for one of its neighbour nodes j. Let $R^i_{est}(j)$ be the value stored in the GRT of i regarding j, and let $R_{rec}(j)$ be a recommendation received from a neighbour different from j.

The new value to store in the GRT will be:

$$R^i_{new}(j) = w_l R^i_{loc}(j) + w_r(w_2 R^i_{est}(j) + w_3 R_{rec}(j)) \quad (2)$$

where w_l, w_r, w_2, w_3 are adequate weights, being $w_l + w_r = 1$ and $w_2 + w_3 = 1$.

For far nodes, for which $R^i_{loc}(j)$ does not exist, the above expression simplifies as follows:

$$R^i_{new}(j) = w_2 R^i_{est}(j) + w_3 R_{rec}(j) \quad (3)$$

In addition to Expression 2, when a node realizes that the reputation of another node has not changed from the previous step, because the observed node is idle or it rejects collaborations, the observer applies the *Old-Age Function*, to decrement the reputation in the GRT. In this way if a node stops collaborating, its reputation decreases over time. In consequence, a node with a good level of reputation is encouraged to maintain a high level of involvement in the packet routing.

A first set of simulations was conducted to find suitable values for the parameters of expressions 2 and 3. The correct choice for them is when the distribution for the reputations stored in the GTRs is sufficiently uniform.

4 Simulation and Performance Evaluation

The entire reputation protocol described above was tested through simulations in order to make the optimal choices for the relevant parameters and ultimately to validate the protocol itself. We used the *Network Simulator 2* (NS2) [11], which is a de-facto standard to analyse network protocols.

NS2 is an event-driven simulator that implements packets, nodes, links, transport and application agents. It provides a reliable structure that allows to model large wired and wireless systems. Also, it implements modules for wireless stations, which can move themselves in a 2D environment. For these stations, NS2 defines some routing protocols, such as DSR, DSDV, AODV [12] and TORA.

The power of NS2 is its flexibility. A user can simply add his own ad-hoc modules to test new protocols. This feature allows us to define some modification to the original DSR agent which turn out to be necessary.

As said before, the first set of necessary tests serves to fix the parameters in the expression 2. The reference scenario is constituted by a network with 24 nodes, distributed in a space of $1000\text{x}800m^2$. Every node has a cover range of $200m$ and is connected with other 6 nodes (see figure 3).

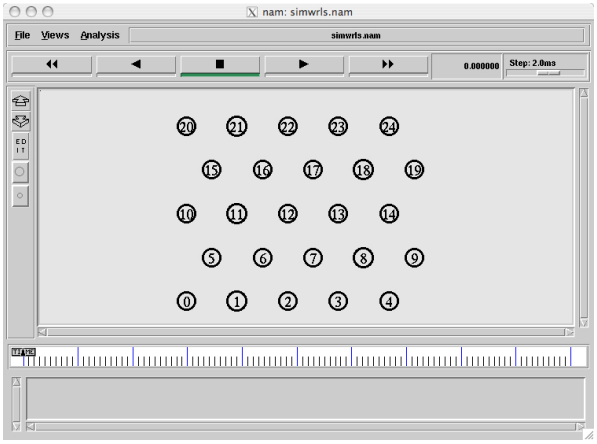

Figure 3. Reference Network Topology

We used the same scenario also to evaluate the distribution of the reputation for a particular node. Figures 4(a) and 4(b) show the trends of the reputation, for a given node,

known by all the others. The first one (fig.a) refers to a source traffic node, so we expect a low reputation value for it. Instead the second one shows the same values referred to a transit node, that does not generate any traffic, but collaborates to the forwarding process. We clearly expect high values for that node.

We were pleased to observe that, after an initial phase, the values converge to a strict bound, with a mean low value in the first case, and a mean high value in the second one.

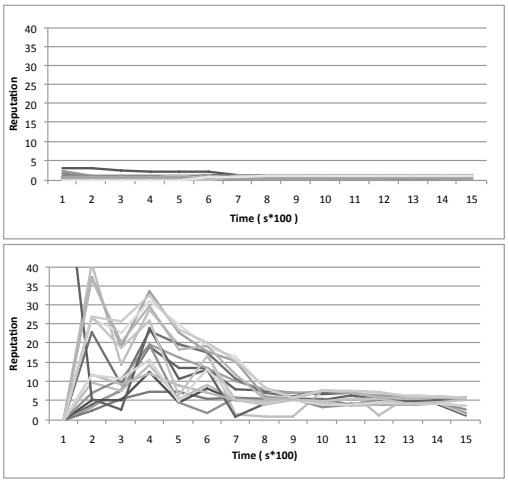

Figure 4. Reputation distribution for a source node and a transit one

It is also significant to check the the spatial distribution of the reputation, which is drawn in Figure 5. The floor of this graph is constituted by the network topology, like in figure 3. Here we highlight only the observed node (node 12) and its one-hop neighbours. As we can see, close nodes have the same value for the reputation. The difference for the zones can be due to the path followed by the communications.

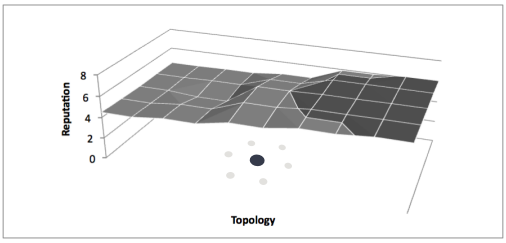

Figure 5. Reputation distribution for a selfish node

The next set of tests was conducted to verify the discovery of selfish behaviour. Let us consider the general case in which an ugly node starts as good and then becomes bad by stopping to forward other nodes' packets. Figure 6 demonstrates the reputation that the network has about such a node. For the sake of presentation, it is convenient to observe the node during its three different states:

- *transient state* has the node start exchanging the GRTs;
- *steady state* has the distribution of the GRTs values almost uniform and the node behaving as good;
- *selfish state* has the distribution of the GRTs values almost uniform and the node behaving as bad; its reputation decreases accordingly.

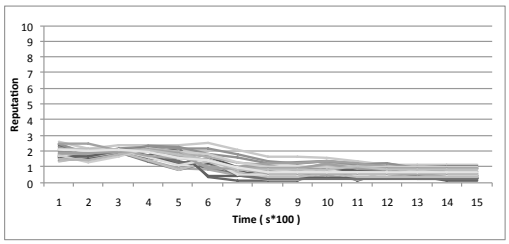

Figure 6. Reputation distribution for a ugly node

Figure 6 omits the transient state because it is not significant due to the fact that the reputation values are not appropriately distributed yet. It can be seen that, when the steady state ends up in the selfish state, the network reputation about the node begins to decrease accordingly. The neighbour nodes experience the decrease at first, and then in turn all other nodes do. The reputation ultimately reaches very low levels. This trend in the simulation supports the claim that our reputation protocol reacts quickly to behavioural changes that indicate routing problems.

5 Conclusions

An open network is composed of nodes without prefixed identity, which do not know each other. In such an environment nodes are attracted by assuming a selfish behaviour, consequently saving battery, energy.

We presented a protocol to allow a node to evaluate the reputation of another one by means of both direct observation and recommendations received from other nodes. Testing our protocol with NS2 confirms that the reputation value calculated by a node can describe with enough accuracy the behaviour of another one.

Our protocol was tested under realistic threats that allow each node to change behaviour and start acting maliciously. Malicious activity in our application domain is any attempt

to subvert the reputation protocol. It therefore translates to acting selfishly by neglecting or ignoring at all the routing of other nodes' packets.

There are various issues that need to be considered in our future research. One concerns collusion of bad nodes that cooperate for the common aim of increasing their reputation. Another crucial issue is the extension of our reputation protocol towards saving the energy of nodes. Power-saving routing is indeed critical for mobile networks in general [13, 14]. Arguably, a viable reputation protocol will help pinpoint the nodes with higher power reserve: these are the selfish ones. More findings can be therefore expected along this research trail.

References

[1] G. Bella, S. Bistarelli, and F. Massacci. Retaliation: Can we live with flaws? In M. Essaidi and J. Thomas, editors, *Proc. of the Nato Advanced Research Workshop on Information Security Assurance and Security*. IOS Press, 2005.

[2] S. Bistarelli and F. Santini. Propagating multitrust within trust networks. In *Proceedings of the 23th Annual ACM Symposium on Applied Computing*, page 5, March 2008.

[3] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation, 2004.

[4] S. Buchegger and J.-Y. L. Boudec. Performance analysis of the CONFIDANT protocol: Cooperation of nodes — fairness in dynamic ad-hoc networks. In *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, June 2002. IEEE.

[5] T. C. Group. Trusted platform model - http://www.trustedcomputinggroup.org/.

[6] D. B. Johnson, D. A. Maltz, and Y.-C. Hu. *The Dynamic Dource Routing Protocol for Mobile Ad Hoc Networks (DSR)*, 2003.

[7] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision, 2007.

[8] J. Liu and V. Issarny. Enhanced reputation mechanism for mobile ad hoc networks. *LNCS*, page 15, 2004.

[9] S. Marsh. Formalising trust as a computational concept, 1994.

[10] P. Michiardi and R. Molva. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, 2001.

[11] The Network Simulator NS-2 - http://www.isi.edu/nsnam/ns/.

[12] C. Perkins. Ad hoc on demand distance vector (aodv) routing, 1997.

[13] C.-Y. Wang, C.-J. Wu, and G. N. Chen. p-manet: Efficient power saving protocol for multi-hop mobile ad hoc networks. In *ICITA '05: Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05) Volume 2*, pages 271–276, Washington, DC, USA, 2005. IEEE Computer Society.

[14] R. Zheng and R. Kravets. On-demand power management for ad hoc networks. In *Proc. IEEE INFOCOM '03*, 2003.