A Novel Approach for Creating Trust to Reduce Malicious Behavior in MANET

Syed S. Rizvi, Saroj Poudyal, Varsha Edla, and Ravi Nepal
Department of Computer Science & Engineering
University of Bridgeport, Bridgeport, CT
(srizvi, spoudyal, vedla, rnepal)@bridgeport.edu

ABSTRACT
This paper presents a Reputation-Trust (RT) system that can be used to stabilize the performance of the network for the working nodes even in the presence of malicious nodes which intentionally do not route and forward packets send by others correctly. The situation becomes even worst when nodes do not rely on any routing infrastructure but relay packets for each other. We introduce two extensions to the Dynamic Source Routing algorithm (DSR) [1] to mitigate the effects of routing misbehavior: the *watchdog* and the *pathrater*. Using these two approaches, the proposed RT system will update the RT table of each node with the ranked values of other nodes. The implementation of the proposed RT system is entirely based on the underlying proposed RT algorithm. Simulation results demonstrate that the RT system can be used to reduce the malicious behavior of mobile nodes and consequently improve the overall performance of MANET.

Keywords
Ad hoc networks, dynamic source routing, reputation trust

1. INTRODUCTION
Ad hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However, a node may misbehave by agreeing to forward packets and then failing to do so. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets.

In this paper, we accommodate extra facilities in the network to detect and mitigate routing misbehavior. In this way, we can make only minimal changes to the underlying routing algorithm. We introduce two extensions to the DSR algorithm to mitigate the effects of routing misbehavior: the *watchdog* and the *pathrater* [1]. The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through these nodes. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening *promiscuously* to the next node's transmissions. If the next node does not forward the packet, then it is misbehaving. The pathrater uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets. The proposed solution could be the use of a self-policing mechanism based on reputation to enable MANET to keep functioning despite the presence of misbehaving nodes. The reputation system in all nodes makes them detect misbehavior locally by observation and use of second-hand information. Once a misbehaving node is detected it is automatically isolated from the network.

CoNEXT'07, December 10–13, 2007, New York, NY, USA.

2. PROPOSED REPUTATION-TRUST (RT) SYSTEM
In order to mitigate the node misbehavior, the Watchdog and Pathrater [1] relies on a method called Reputation System. However, we propose a new RT system and an underlying RT algorithm which works in a local network environment on top of the existing Watchdog and Pathrater systems. When compare with the global reputation based schemes, such as CONFIDANT [2] and CORE [3], the proposed RT system uses local reputation. Each node in RT system maintains a table with trust and reputation values of all local nodes. When misbehavior of nodes is found, the RT System becomes active and starts updating all the table info based on the information provided by its neighbor as well as by Watchdog.

2.1. Proposed Model for the RT System
In our proposed RT system, trust in a node is associated with its reputation value. There are only two discrete levels of trust. Symbol ${}_AT_B$ is used to represent the trustworthiness of node *A* on node *B*. A node *A* considers another node *B* either:

- To-be-Trusted with $T = 1$,
- Not-Trusted, with $T = 0$

A *To-be-Trusted* node is a well behaved node and nodes trust this with depth of its reputation value. A *Not-Trusted* node is a misbehaved node and should be avoided and deprived of services. When a new node is entered in the network, it is assumed to be trustworthy with *T=1* and Reputation *R=1* as well. Its future performance decides its true Trust and Reputation value. Every node keeps a reputation table, which associates a reputation value and its trust level with each of its neighbors. It updates the reputation table based on the algorithm defined below. Reputation values *R* are between a range 0< R < 1, and there are two thresholds:

- T_L below which the node is said to be *Not-Trusted*.
- T_H above which the node is said to be *Trusted*.
- So *R* has a Range ($0 <= T_L < T_H <= 1$)

The proposed RT system uses its RT table to find the Trust and Reputation so that it can update the values accordingly.

2.2. Proposed RT Algorithm

Suppose node *S* wants to calculate the reputation of a node *D* in its table *RT(S)* which is not an immediate neighbor of *D*. Let *I* is any intermediate node which follows 2 conditions: Node *S* trust node *I* ($_S T_I = 1$) and Node *S* knows Reputation of node *I* (R_I is known). If *L* is a total amount of data entering node *D* and L_O is load exiting node *D*, with total network being *W*. Then Reputation of node D is: Improved ($R_D < L_O / L$) and Misbehaved ($R_D > L_O / L$). Load factor for node *D* is: L_O/W , the new Reputation results:

$$\xrightarrow{Improved} R_D = R_D + (L_O/L)\times(L_O/W) = R_D + (L_O)^2/LW$$

$$\xrightarrow{Misbehaved} R_D = R_D - (L_O/L)\times(L_O/W) = R_D - (L_O)^2/LW$$

3. PERFORMANCE ANALYSIS

Fig. 1 shows a network that consists of 10 connected nodes. The dark line shows that the nodes trust each other whereas the dotted line shows that nodes do not trust each other. The value given is for the reputation of one node over others. As shown in Fig. 2, all the nodes in the path from source (S) to *D* via *A* are behaving good as their reputations are higher (close to 1.0). This implies that the path raters rating for the path is typically 0.84 as shown in

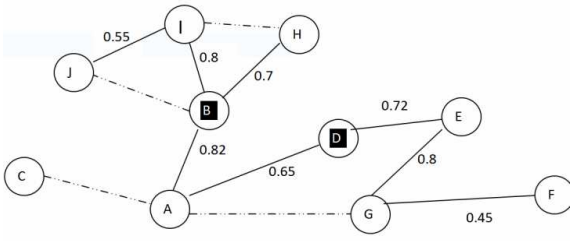

Fig.1 Nodes with trust and reputation

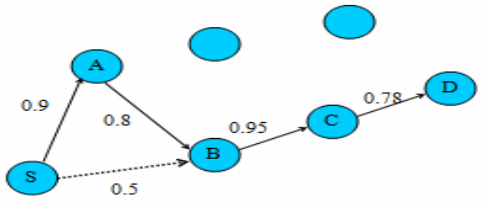

Fig.2. Scenario I

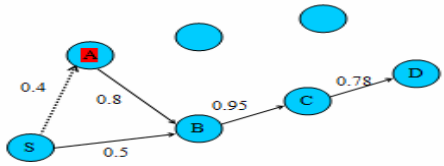

Fig.3. Scenario II

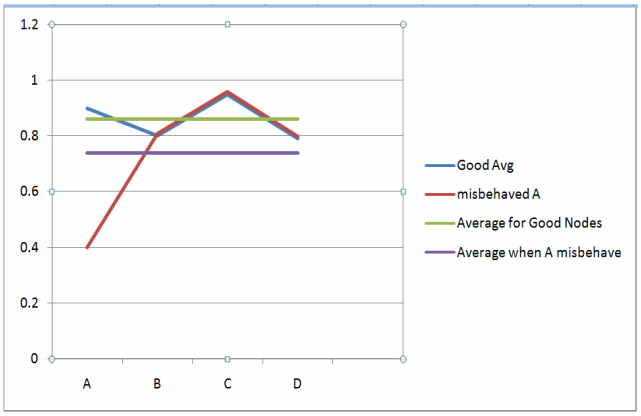

Fig.4. Reputation and Path rating

Fig. 4. It should be noted in Fig. 3 that all nodes are well behaved except node *A*, the RT Algorithm hence have dropped the reputation of *A* to 0.4, which results in drop in path rate close to 0.74 as shown in Fig. 4.

4. CONCLUSION

We concluded that even if only single node is misbehaving in a good path, the overall rating of the path drops drastically, so other good node will try to avoid this bad node in their path, which results in selecting a good neighbor and bad node is isolated from the path.

5. REFERENCES

[1] K. Lai, and M. Baker, S. Marti, T. Giuli, "Mitigating routing Misbehavior in mobile Ad hoc networks," *in Proceedings of MOBICOM 2000*, pp. 255–265, 2000.

[2] S. Buchegger and L. Boudec, "Performance analysis of the confidant protocol," *in Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, pp: 226-236, 2002.

[3] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node Cooperation in mobile Ad hoc networks," *Sixth IFIP conference on security communications, and multimedia (CMS 2002)*, Portoroz, Slovenia, 2002.