A Fuzzy Reputation System in Vehicular Ad hoc Networks

Mohammad Jalali\textsuperscript{a} *, Nasser Ghasem Aghaee\textsuperscript{b},

\textsuperscript{a}Department of computer engineering, University of Isfahan, Isfahan, Iran
\textsuperscript{b}Department of computer engineering, University of Isfahan, Isfahan, Iran

Abstract

Vehicular Ad hoc Networks (VANET) rely on the cooperation of the nodes to forward packets for each other. Some nodes may decide not to cooperate to save their resource while still using network resources. These nodes are called selfish. It has been shown that presence of such selfish nodes degrades the overall performance of a vehicular ad hoc network.

To address this problem, we propose a fuzzy reputation system to discipline selfish behavior and encourage packet forwarding. Different from traditional reputation based solutions, our scheme doesn't rely on judgments about a node by its neighbors. So the misjudgments about a node which is a serious vulnerability in existing solutions have been eliminated. Our solution consists of two major components: The Forward Manager and the Fuzzy Reputation Manager. The Forward Manager in each node keeps track of the number of received forwarding requests and the number of packets which have been forwarded so far. The Fuzzy Reputation Manager checks each packet's source node to see whether it is selfish or not. Packets belong to selfish source nodes eliminate from the network.

The simulation results have shown that the proposed scheme can successfully increase network performance.

Keywords: Vehicular Ad hoc Networks; Selfish behavior; fuzzy reputation; cooperation enforcement

1. Introduction

Vehicular Ad hoc networks (VANET) are special cases of mobile ad hoc networks (MANET), in which nodes (vehicles) cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. Currently routing protocols for VANET are based on the assumption that all nodes cooperate. However, cooperation is not always guaranteed. In VANET, the nodes are not belong to a single authority and they do not pursue a common goal. Nodes that do not cooperate are called selfish. Selfish nodes can be serious problem for VANET and reduces its performance.

Many schemes have been proposed to address this problem in MANET [1-5]. Solutions that stimulate cooperation in mobile ad hoc networks can be categorized as virtual currency based schemes and reputation based schemes. Virtual currency schemes use some form of stimulus to enforce node’s cooperation. Nodes get the
incentives upon serving the network and use these to gain service from the network. If a node does not have any incentives, it will not get any service from the network. In reputation based schemes, on the other hand, nodes maintain the reputation of other nodes based on direct observation or the exchange of reputation messages with other nodes. The basic problem with virtual currency based schemes is they suffer from the location privilege problem [6]. Nodes in different locations of the network will have different chances for earn virtual currency. Besides, some virtual currency based solutions require a central server to determine the charge and credit to each node (as in Sprite [5]). These solutions may not be truly decentralized. Reputation based schemes categorized in two distinctive groups:

- First-hand reputation schemes in which a node get reputation information by direct observations. For example, node A forwards a message to its next hop, B, and expects B to further forward the message. Node A can get first-hand information by monitoring whether B correctly participates in the protocol.
- Second-hand reputation schemes work based on reputation information received from other nodes. Such reputation information can be in the form of a blacklist, friend list, or a reputation table [7].

2. Related work

To stimulate cooperation among selfish nodes in VANET, several solutions have been proposed [9], [10] and [11]. Ho. et al. used a three counter (3C) module (Forward Request Counter, Forward Counter and Location Discover Counter) in each node [9]. When a source node want to send a packet, the source node’s 3C module adds the 3C’s header to the packet and based on this header its neighbors can decide to forward or discard source node’s packet. Li and Jie in [10] proposed FRAME, a virtual currency based solution in vehicular networks for cooperation enhancement. Their rewarding scheme is based on number of direct sprays and the time period that a node stores a packet. Authors of [11] made use of virtual currency scheme to mitigate selfish behavior. In this solution, when a packet reaches the destination, each node that participated in the forwarding should report its contribution to the source node. The final contribution is calculated through the sum of the partial contribution of each node in the forwarding tree. Each intermediate node will receive a reward based on final contribution and number of relay nodes. Vehicle Ad-Hoc Reputation System (VARS) uses direct and indirect reputation as well as opinion for packet forwarding [12].

3. Our scheme

In this paper, we propose a fuzzy reputation system in vehicular networks based on the following assumptions:

- When we talk about node it means vehicle and vice versa.
- No malicious node exists in the network.
- A solution should be completely decentralized.
- Nodes move at a high average speed.
- There is no collusion between selfish nodes in the network.

We also assume that there are three tamper-proof counters in each vehicle (Forward Request counter, Forward Counter and Discard Counter) similar to 3C module in [9]. When a source node sends a packet, these counters are added to packet’s header. Based on these values, relay nodes can decide whether to forward or discard the packet.

Our solution consists of the following components: The Forward Manager and the Fuzzy Reputation Manager.

3.1. The Forward Manager

The Forward Manager has two tamper-proof counters:

- Forward Counter: When a node forwards a packet, its Forward Manager adds forward counter.
- Forward Request Counter: If a node receives a forward request for a packet which is not duplicated, the Forward Manager increases forward request counter.

The Forward Manager adds these counters to every packet which the node wants to send as a source node. These counters are used to determine whether a node is misbehavior or not. If a node’s forward request counter is much more than its forward counter, we can assume that this node is selfish. Because these counters are inside the source node, this judgment should be nearly true. Compared to traditional reputation systems, which are based on other
nodes’ judgments and we know their judgments are not true all the time, since the watchdog mechanism can be wrong because of link breakage. In VANET - since their topology changes rapidly - these link breakages occur occasionally.

We assume that there is no malicious node in the network and this means the counter values would not change by other nodes. Also we assume that there is no collusion between nodes and so no node changes counter values of another node to hide its misbehavior.

### 3.2. The Fuzzy Reputation Manager

Because there isn’t a strict boundary between good and bad behavior, we use a fuzzy reputation manager in each node. The fuzzy reputation manager uses Forward Counter and Forward Request Counter values (F and FR respectively) to decide to forward or discard packets from a source node. When node i receives a packet which node j is its source, based on j's counters node i calculates:

\[ \Theta = \frac{F}{FR} \]  

We introduce \( \Theta \) in terms of fuzzy sets and their ranges as illustrated in figure 1.

![Membership function of fuzzy variable (\( \Theta \))](image)

This fuzzy variable varies from 0 to 1. Low value is represented by values between 0 and \( \Theta_2 \) and high value is between \( \Theta_1 \) and 1. Later in Simulation Study section, we will use \( \Theta_1 \) and \( \Theta_2 \) as simulation parameters to discuss about their influences on vehicular network.

It is obvious that \( \Theta \) indicates node’s behavior. Low value means misbehavior and high value means good behavior. Based on \( \Theta \), relay nodes can judge about source nodes' behavior. Now we should represent fuzzy rules to reflect these judgments. Since we have one variable and it has two linguistic values, there must be two fuzzy rules:

**Fuzzy Rule 1:** IF \( \Theta \) is low THEN discard packet.

**Fuzzy Rule 2:** IF \( \Theta \) is high THEN forward packet.

Note that if node i discard a packet of node j due to j’s misbehavior, forward request counter of node i increases and its forward counter stay unchanged and therefore the fuzzy variable (\( \Theta \)) of node i decreases. This is not our interest because node i does not show misbehavior and its \( \Theta \) must stay unchanged. To solve this problem we use a tamper-proof Discard Counter in the fuzzy reputation manager which counts discards due to source nodes' misbehavior. The Fuzzy Reputation Manager adds this counter to every packet which the node wants to send as a source node. So (1) should change as follows:

\[ \Theta = \frac{F+D}{FR} \]  

Where D indicate discard counter value.

Initial value for \( \Theta \) should be high, due to a recently joined node which does not receive any forward request is not identified selfish by relay nodes.

### 4. Simulation study

#### 4.1. Simulation setup

All simulations are carried out on NS2 [13]. We setup the simulation in a 2000 by 2000 meters area. We use VANET mobility model [14] to generate vehicles’ mobility traces. Experiments are based on a mobile ad hoc network with 300 nodes. Each node has a radio range of 200 meters. Constant bit rate is the application used for
connections and 1/20 of all nodes involve into sessions. Packets are 2 Kbytes. The experiments repeated 200 times per setup with different seed numbers and collected data were averaged over those runs.

4.2. Experimental results

Figure 2 shows the effect of three different pair of $\Theta_1$ and $\Theta_2$ on goodput of the network based on percentage of selfish nodes. In scenario1 we choose $\Theta_1$ and $\Theta_2$ near and toward 100% and as a result, relay nodes are fastidious with source nodes. In scenario2 $\Theta_1$ and $\Theta_2$ are near and toward 0%, so relay nodes are lenient. In scenario3 $\Theta_1$ and $\Theta_2$ are far apart. As you can see in figure 2, for low and high percentages of selfish nodes, lenient relay nodes - scenario1 - implies higher goodput.

![Figure 2. Goodput expressed as the ratio of received to sent packets for three scenarios.](image1)

The performance of our solution in comparison with defenseless scheme for varying percentage of selfish nodes is depicted in figure 3. The reason that in the absence of selfish nodes the mean receive ratio is below 100% is that losses are not only due to selfish nodes dropping packets but also to link errors or because nodes have moved away too quickly and cause link breakages.

![Figure 3. Comparison between defenseless network and our solution based on percentage of selfish nodes.](image2)

Figure 4 indicates the network throughput converges by using our solution. Clearly more percentages of selfish
nodes results in fewer final throughput but has no effect on convergence time (near 700 seconds). On the other hand, changes in percentage of selfish nodes do not make the behavior of the network unstable.

Delay is one of the most important performance measurements for any wireless network system. It represents the average time duration of a packet transmitting from a source node to the destination. In order to reduce the delay, the optimal situation is, all nodes along the route can forward the packet immediately until it reaches the destination. In our scheme, each packet needs to be checked if its source is misbehavior or not and this could cause a delay in packet forwarding process. From figure 5, it can be seen that the imposed delay by our solution is negligible in comparison with defenseless scheme.

5. Discussion

This section presents some advantages of our solution over traditional reputation based schemes.

- Every node has its reputation with itself! So unlike other techniques, misjudgments of other nodes do not isolate a node.
- In second hand reputation based systems each node exchanges its beliefs about other nodes. Disseminate reputation information greatly increases the volume of network traffic. Consider vehicular ad hoc networks, where bandwidth is limited, this is an important issue. In our work the overhead is three fields added to every
packet.

- Inconsistent reputation value is another issue which reputation based schemes are faced with. In reputation systems, different nodes may have different reputation values for one node. In our solution, each node reports its behavior to others. So all nodes have same belief about its reputation value.

- We believe that there is no strict boundary between good and bad behavior. Therefore unlike other reputation systems, we use a fuzzy reputation manager to handle this fact.

- Unlike many techniques that avoid selfish nodes during routing and forwarding procedures, the Fuzzy Reputation Manager of non-selfish nodes allows selfish nodes to cooperate in routing and forwarding packets and so they can increase their reputation and join the network again.

6. Conclusion and future work

In this paper, we proposed a fuzzy reputation system to mitigate selfishness in VANET. In our solution, behavior of each node calculated in itself by two tamper-proof counters. Therefore misjudgment about nodes which is a troublesome problem in traditional solutions has been solved. We first defined the system and its components and then we introduced the fuzzy variable and fuzzy rules.

In simulation study, we showed that using our scheme, increases network performance in the presence of selfish nodes. In addition, simulation studies implied that regardless of the number of selfish nodes, network throughput converges. On the other hand, our solution makes network throughput stable.

In the future, we plan to investigate how to define the membership function of fuzzy variable reasonably and properly to achieve best performance.

References