A Distributed Reputation Management Method for Vehicular Ad Hoc Networks

Chun-Liang Lee*, Yang Chen*, Yu-Rang Huang*

*Department of Computer Science and Information Engineering, School of Electrical and Computer Engineering, College of Engineering, Chang Gung University, No. 259, Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan 33302, Taiwan

*Corresponding Author: clee@mail.cgu.edu.tw

Abstract

Vehicular ad hoc networks (VANETs) have attracted a lot of attention in recent years. Possible applications include car accident notification, emergency vehicle warning systems, and real-time traffic information sharing. These applications require each network node (i.e., vehicle) to share its own information with other nodes, and to forward packets sent by other nodes. However, a misbehaving node may refuse to forward packets or modify arriving packets before forwarding it. One promising solution to this problem is to use reputation management systems, which can detect misbehaving nodes. In this paper we describe our proposal for a distributed reputation management system for VANETs. Compared with centralized reputation management systems, our proposed system is more scalable and suitable for VANETs. In our proposed system, a node calculates reputation values of its neighboring nodes by monitoring exchanged packets, and shares the information of its neighboring nodes with low reputation values with other nodes. Since all control packets are limited in a certain range, the communication overhead is marginal. Experimental results indicate that our proposed system achieves up to 11% higher packet delivery ratio compared to the T-GPRS protocol.

Keywords: vehicular ad-hoc networks, reputation management systems.

1. Introduction

With the fast advances in wireless communication technologies, mobile ad hoc networks (MANETs) have drawn great attention in recent years. In MANETs, nodes can build a temporary network for communication without any fixed infrastructures. If mobile nodes are vehicles, this type of network is called vehicular ad hoc network (VANET). VANETs differ from MANETs in several aspects. The most notable one is that vehicles move only on predetermined roads rather than randomly moving. Another difference is that vehicles move much faster than nodes in MANETs, resulting in fast topology changes in VANETs. With the help of VANETs, each driver or each vehicle can share information with others through inter-vehicle communications, which provides drivers new features and applications. For example, emergency events can be propagated among vehicles to avoid a multicar chain accident. Drivers can change their route plans according to the traffic information received.

The success of VANETs greatly relies on all vehicles to share their information and transmission capabilities. A misbehaving node may damage the whole system through two ways. First, it may be a selfish node which receives packets from other nodes, but refuses to forward the packets to other nodes for saving its own energy. A selfish node is less harmful to the system, but may reduce the efficiency of packet dissemination in the network. Second, a misbehaving node may distribute faulty information by modifying packets received from other nodes. This causes severer negative impact on the network than selfish nodes.

In order to mitigate the damage that misbehaving nodes may cause to the network, reputation management methods have been proposed in the literature. A reputation management system provides two major functions. First, it helps nodes identify misbehaving nodes by evaluating node reputation. Second, based on node reputation, a node can discard packets sent from nodes with low reputation values. This not only can isolate misbehaving nodes from the network, but also prevent corrupted packets from spreading...
in the network. In addition, if source routing protocols are used, a node can construct a route that consists of only nodes with high reputation values. This can avoid routing packets through misbehaving nodes, and thus increases the packet delivery ratio.

Due to the importance of reputation management, a number of proposals can be found in the literature. Most of them were based on centralized approaches, which require nodes to send reputation-related information to a centralized server through road-side units (RSUs). The centralized server is responsible for collecting the information, processing, and deriving the reputation value for every node. The major advantage of the centralized approach is that it is simple and can correctly identify misbehaving nodes. However, it requires support from the network infrastructure. That is, the coverage of RSUs must be large enough; otherwise, the centralized server may fail to obtain enough information to calculate node reputation. In addition, the centralized approach suffers from the scalability problem. Therefore, in this paper, we propose a distributed reputation management method which is more scalable and suitable for VANETs than centralized approaches. With our proposed method, a node calculates reputation values of its neighboring nodes by monitoring exchanged packets, and shares the information of its neighboring nodes with low reputation values with other nodes. Since all control packets are limited in a certain range, the communication overhead is marginal.

The rest of this paper is organized as follows. Section 2 briefly reviews the literature related to this work. Section 3 presents our proposed reputation management system. Section 4 shows experimental results and discussion. Finally, a conclusion is drawn in Section 5.

2. Related Work

In order to increase network throughput, Marti et al. proposed two techniques: watchdog and pathrater. The watchdog detects misbehaving nodes by monitoring the behaviors of neighboring nodes. Suppose that node A wants to send a packet to node C through node B. Once node A sends out the packet, it can monitor node B’s traffic. If node B does not forward the packet in a certain amount of time, node A will conclude that node A is a selfish node. In addition, if node B forwards the packet with corrupted payload, node A will conclude that node A is a misbehaving node. The pathrater rates each node based on the information from the watchdog, and then helps routing protocols avoid nodes with low rating. However, the pathrater does not punish misbehaving nodes, but rather relieved of the burden of forwarding packets for others.

Buchegger and Boudec proposed a protocol called CONFIDANT, which detects and isolates misbehaving nodes. The CONFIDANT protocol improves the disadvantage of the watchdog and pathrater mentioned above. Michiardi and Molve proposed a mechanism named CORE to enforce node cooperation based on a collaborative monitoring technique. The major difference between the CORE mechanism and the pathrater technique is that the CORE mechanism stimulates misbehaving nodes to contribute the network. In contrast, the pathrater isolates misbehaving nodes from legitimate nodes.

The above mentioned protocols are based on on-demand routing protocols, such as DSR and AODV. An on-demand routing protocol, as its name says, finds a route from the source to the destination when transmission is required. Karp and Kung proposed the Greedy Perimeter Stateless Routing (GPSR) protocol, which uses geographical positions of nodes for routing messages. Prizada and McDonald proposed an improved variant of the GPSR protocol called Trusted Greedy Perimeter Stateless Routing (T-GPSR) protocol that computes the trust level of a node using an effort-return based trust model. Their simulation results indicate that compared to the GPSR protocol, T-GPSR can achieve 30% higher packet delivery ratio than the GPSR counterpart when the misbehaving node percentage is 50%.

3. Proposed Distributed Reputation Management Method

3.1 Watchdog

Similar to that used in our proposed method uses a watchdog component for monitoring the behaviors of neighboring nodes. Once a node transmits a packet, it keeps the packet in a buffer for a period of time \(t_b\), and monitors its neighboring node that should forward the packet toward the destination. If the monitored node does not forward the packet in \(t_b\), a timeout event \(e_{to}\) will be triggered. If the monitored node forwards the packet, the original node will check if the packet was modified. If so, a corruption event \(e_c\) will be triggered. If the monitored node forwards the packet without modifying, a forwarding completion event \(e_{fc}\) will be generated. The three events mentioned above also perform a reputation update, which will be describe in
3.2 Reputation Management

As described in the last subsection, once an event is triggered, reputation update will be executed. To keep reputation assessment about neighboring nodes up-to-date and to save storage, a node stores the latest $K$ events for each neighboring node. Once a new event is triggered, since the event contains the identifier of the involving node, say $n$, the oldest event regarding node $n$ will be replaced by the new event. Let $e_i$ denote the latest event, and $e_K$ the oldest event. The reputation value of $r_n$ is calculated using the following equations:

$$w_i = \frac{w - (1 - w)^i}{\sum_{j=1}^{K} w - (1 - w)^j} \quad (1)$$

$$r_n = \sum_{i=1}^{K} w_i * \text{value}(e_i) \quad (2)$$

, where $w$ is a system parameter with values ranging between 0 and 1. Function $\text{value}(e_i)$ returns a value according to the type of $e_i$, and is defined as follows:

$$\text{value}(e_{TO}) = -1 \quad (3)$$

$$\text{value}(e_{DC}) = -1 \quad (4)$$

$$\text{value}(e_{FC}) = 1 \quad (5)$$

$$\text{value}(e_{AD}) = -0.5 \quad (6)$$

Equation (1) has two important features:

(a) For any value of $K$, the sum of $w_1$ to $w_K$ is 1.

(b) The value of $w_i$ decreases with increases of $i$.

Thus, Equation (2) calculates the reputation value of a node by putting more weight on recent events than on old events. Based on Equations (1) and (2), reputation values are between -1 and 1.

3.3 Forwarding Node Selection

After calculating reputation values of neighboring nodes, a node classifies its neighboring nodes into three categories:

(a) Well-behaving nodes: nodes with a reputation value larger than $T_w$.

(b) Misbehaving nodes: nodes with a reputation value smaller than $T_m$.

(c) Natural nodes: nodes with a reputation value between $T_m$ and $T_w$.

Once a node wants to transmit a packet, it first selects an adjacent neighbor that has the least distance to the destination, and is classified as well-behaving nodes. If there is no such node, it then checks those nodes classified as natural nodes. Finally, it checks those nodes classified as misbehaving nodes. Since a node selects a forwarding node not only by its geographical position, but also by its reputation value, the packet delivery ratio can be increased by reducing the possibility of being dropped by misbehaving nodes.

4. Experimental Results

4.1 Setup

The simulation of our proposed reputation management method was performed using the ns-2 network simulator\textsuperscript{10}. Vehicular movement traces were generated by the VanetMobiSim simulator\textsuperscript{11}. Table 1 lists the simulation parameter settings. Figure 1 shows the road topology we used to evaluate our proposed method. We generated a total of six vehicular movement traces. For each vehicular movement trace, five simulation tasks were performed. For each simulation task, ten connections were established.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network simulator</td>
<td>ns-2 v2.34</td>
</tr>
<tr>
<td>Area of map</td>
<td>3000 * 3000 m(^2)</td>
</tr>
<tr>
<td>MAC protocol</td>
<td>IEEE 802.11p</td>
</tr>
<tr>
<td>Transmission range</td>
<td>300 m</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR (UDP)</td>
</tr>
<tr>
<td>Number of connections</td>
<td>10</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Vehicle density</td>
<td>30 cars/km(^2)</td>
</tr>
<tr>
<td>Vehicle speed</td>
<td>8.33 – 13.89 m/second</td>
</tr>
<tr>
<td>Simulation time</td>
<td>900 seconds</td>
</tr>
<tr>
<td>Transmission range for warning packets</td>
<td>500 m</td>
</tr>
<tr>
<td>$T_w$</td>
<td>0.1</td>
</tr>
<tr>
<td>$T_m$</td>
<td>-0.1</td>
</tr>
<tr>
<td>$w$</td>
<td>0.1</td>
</tr>
<tr>
<td>$K$</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 1. Simulation parameter settings.

Results for the effects of misbehaving node percentage on packet delivery ratios (PDR) are shown in Figure 2. PDR is defined as the number of packets received by...
destination nodes divided by the number of packets transmitted by source nodes. Our proposed method achieved higher PDRs than the GPSR and T-GPSR methods. When there were no misbehaving nodes (i.e., misbehaving vehicle percentage = 0%) in the network, all methods achieved an identical PDR. When the misbehaving vehicle percentage was increased from 0% to 10%, our method achieved 8% higher PDR than the T-GPSR method, and 16% higher PDR than the GPSR method. PDR improvement for our method was further enhanced when the misbehaving vehicle percentage was increased from 10% to 20%. The reason is that when the misbehaving vehicle percentage was 10%, it was easier for other methods to select a non-misbehaving vehicle even reputation was not considered. However, when the misbehaving vehicle percentage was 20%, it was harder; thus, more packets were dropped by misbehaving vehicles, as shown in Figure 3. When the misbehaving vehicle percentage was 30% or larger, PDR improvement for our method began to decline. This is because when the misbehaving vehicle percentage was too large, it was hard for a vehicle to find an adjacent vehicle that was a well-behaving vehicle.

5. Conclusions

In this paper, we proposed our proposal for a distributed reputation management system for VANETs. Compared with the GPSR and T-GPSR methods, our proposed methods selects a forwarding node according to not only geographical positions of nodes, but also reputation values. Since broadcasted messages are limited in a certain range, our proposed method does not incur much communication overhead. According to our results, our proposed method can achieve higher PDRs than the other tested methods.

Acknowledgment

This work was supported in part by the High Speed Intelligent Communication (HSIC) Research Center of Chang Gung University, Taiwan, and by grants from the Ministry of Science and Technology of Taiwan (NSC 99-2221-E-182-053 and MOST-104-2221-E-182-005) and Chang Gung Memorial Hospital (BMRP 942).

References


