International Journal of Innovative Computing, Information and Control
Volume **13**, Number **2**, April **2017**

ICIC International ©2017 ISSN 1349-4198
pp. 535–546

REPUTATION MANAGEMENT FOR EFFICIENT MESSAGE TRANSMISSION IN VEHICULAR AD HOC NETWORKS

Chun-Liang Lee*, Yang Chen and 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: cllee@mail.cgu.edu.tw; {M0329010; M9829013}@stmail.cgu.edu.tw

Received August 2016; revised December 2016

Abstract. *In vehicular ad hoc networks (VANETs), individual vehicles can share information and resources in support of useful applications such as real-time traffic navigation, emergency vehicle warning systems, and car accident notification. A key factor in VANET application success is good behavior on the part of each network node – that is, every node (vehicle) must share information and resources. In this paper we describe a reputation management system for detecting poorly behaving nodes in order to isolate them from properly performing nodes. Since our proposed system is fully distributed (i.e., lacks a centralized control node), it is more scalable and suitable for VANETs. In our proposed system, nodes monitor packets that are forwarded to their neighboring nodes, and use gathered information to calculate reputation values for each neighbor. These values are used to identify and select forwarding nodes, and to notify neighbors about the presence of nodes with low reputation values. Results from experiments indicate that our proposed system is capable of achieving a packet delivery ratio that is 10% higher than that produced by the T-GPSR protocol, with low communication overhead.*
Keywords: Vehicular ad hoc networks, Reputation management systems, Cooperation

1. **Introduction.** Vehicular ad hoc networks (VANETs) are currently the focus of considerable research attention [1, 2, 3, 4, 5, 6, 7]. Similar to mobile ad hoc network (MANET) nodes, VANET nodes can communicate with each other in the absence of fixed infrastructures. However, VANETs differ from MANETs in several ways, perhaps the most important being that VANET nodes (vehicles) can only move along predetermined routes [8]. Another significant difference is that VANET vehicles move much faster than MANET nodes, thus producing rapid topological changes. VANETs support the sharing of information and resources with other vehicles via inter-vehicle communication, allowing for the implementation of novel and useful purposes such as real-time traffic reports-plus-navigation software for determining optimum routes. Another example is the immediate broadcasting of accidents in order to prevent chain collisions.

In the absence of a fixed infrastructure, VANET success is greatly dependent on the sharing of information among nodes. However, there is a likelihood of some nodes being uncooperative, resulting in two possible types of damage to an entire system. First, a selfish node may receive packets from other nodes, but refuse to forward them in order to conserve energy or bandwidth. While selfish nodes may be less harmful to a system, they reduce message dissemination efficiency. Second, a misbehaving node may distribute faulty information by modifying messages received from other nodes, triggering much greater negative impacts than selfish nodes. In order to mitigate the network damage

caused by misbehaving nodes, researchers have proposed several reputation management methods that serve two primary functions: evaluating node reputations to assist in misbehaving node identification, and using node reputation information to discard suspect packets sent by low-reputation nodes [9]. Further, source routing protocols can help nodes construct routes consisting of high-reputation nodes only, thus blocking the routing of packets via misbehaving nodes, and increasing packet delivery ratios.

Most of the reputation management proposals in the literature are based on centralized approaches that require nodes to send reputation-related information to a central server via road side units (RSUs) [10, 11, 12, 13, 14, 15]. The server is responsible for collecting and processing information that is used to determine each node's reputation value. The major advantages of centralized approaches are their simplicity and capability to correctly identify misbehaving nodes. However, support is required from the network infrastructure: RSU coverage must be sufficiently large; otherwise the central server may not have enough information for the node reputation calculation task. Centralized approaches also suffer from scalability and robustness problems. Specifically, server storage and computing capabilities limit the maximum number of nodes that can be supported. In addition, servers are susceptible to breakdowns caused by accidental or malicious problems, thus triggering reputation system failures. We, therefore, created a distributed reputation management method that is more scalable and suitable than centralized approaches for VANETs, with nodes calculating the reputation values of neighboring nodes by monitoring packet exchanges, and sharing information about nodes with low reputation values. Since all control packets in our proposed system are limited to specific ranges, communication overhead is low.

The rest of this paper is organized as follows. A brief review of the literature on this topic is presented in Section 2, details regarding our proposed reputation management system are given in Section 3, experimental results are presented and discussed in Section 4, and a conclusion is offered in Section 5.

2. **Related Work.** To increase network throughput, Marti et al. [16] have proposed two techniques that they call "watchdogs" and "pathraters". Watchdogs detect 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 the packet, it can monitor all packets sent by node B, and identify node B as *selfish* if it does not forward the packet within a certain amount of time. If node B forwards the packet but with a corrupted payload, A will conclude that B is a *misbehaving node*. In contrast, pathraters rate each individual node based on information from watchdogs, and then use routing protocols to block nodes with low ratings. Pathraters do not punish misbehaving nodes, but instead relieve them of the burden of forwarding packets.

Two proposals are of particular interest to the present study. Buchegger and Boudec [17] have created a protocol called CONFIDANT that both detects and isolates misbehaving nodes. The CONFIDANT protocol consists of four components: a monitor, trust manager, reputation system, and path manager. The function of the monitor is similar to that described above for the watchdog – that is, detecting deviations from normal routing behaviors. The trust manager handles incoming and outgoing alarm messages, which are used to warn others about malicious node activity. The reputation system rates other nodes based on their behaviors. The path manager maintains path rankings and responds to paths that contain misbehaving nodes. Michiardi and Molva's [18] CORE mechanism uses collaborative monitoring to enforce node cooperation. The major difference between

the CORE mechanism and the pathrater technique is that the first stimulates misbehaving nodes to contribute to networks, while the second isolates misbehaving nodes from legitimate nodes.

All of the above-mentioned techniques use on-demand routing protocols such as dynamic source routing (DSR) [19] and ad hoc on-demand distance vector (AODV) routing [20]. As their names suggest, these types of protocols identify the best routes from sources to destinations when transmission is required. Another protocol known as greedy perimeter stateless routing (GPSR) uses the geographic positions of nodes to route messages [21]. Each node periodically uses beacons to inform adjacent nodes about its current position, information that can be used in support of packet forwarding. Thus, when a node receives a message, it identifies the node that is the closest to its destination.

One shortcoming of GPSR is that it does not account for misbehaving nodes when selecting a forwarding node. Pirzada and Mcdonald [22] have proposed a GPSR protocol variant that they named "trusted greedy perimeter stateless routing" (T-GPSR) that uses an effort-return trust model to compute node trust levels [23]. Their simulation results indicate that compared to GPSR, T-GPSR achieved a 30% higher packet delivery ratio (PDR) when the misbehaving node percentage was 50%. However, T-GPSR only uses events that have been directly experienced by a node to calculate reputation values, which may slow down the misbehaving node identification process. Our strategy for overcoming this problem is to use indirect reputation values shared by other nodes when performing reputation calculations.

3. **Proposed Distributed Reputation Management System.**

3.1. **Reputation-related event collection.** Node reputation values are determined by their behaviors. To monitor the behaviors of neighboring nodes, our proposed system uses a watchdog component similar to that described in [16, 18]. When a node n transmits a packet, it retains the packet in a buffer for a period of time (t_f) while monitoring a neighboring node that is supposed to forward the packet toward its destination. A timeout event (denoted as e_{TO}) is triggered if the monitored node does not forward the packet within t_f. If the monitored node does forward the packet, node n checks to determine if the packet was modified; a corruption event (denoted as e_C) is triggered if it finds positive evidence to that effect. If the monitored node forwards the packet without modifying the content, a forwarding completion event (denoted as e_{FC}) is generated. Each of the three events entails a reputation update (to be described in detail in the following subsection). If the updated reputation value is smaller than a threshold T_m, node n broadcasts a warning packet containing information about its geographic position along with a low-reputation node identifier. When a node receives a warning packet, it immediately determines if the geographic position is within or beyond a predefined transmission range (r_w). If it is beyond, it discards the warning packet; otherwise, it rebroadcasts the packet and triggers a warning event (denoted as e_W).

3.2. **Reputation management.** To save storage and to keep reputation assessments of neighboring nodes up-to-date, a node in our proposed system only stores the most recent K events for each neighboring node. Since each event contains the identifier of the node involved (labeled as n in this example), when a new event is triggered, the oldest event involving node n is replaced by the more recent event. Let e_1 denote the latest event and e_K the oldest event. Function $value(e)$ returns a value according to the event e type, defined as

$$value(e_{FC}) = 1 \tag{1}$$

$$value(e_{TO}) = -1 \tag{2}$$

$$value(e_C) = -1 \tag{3}$$

$$value(e_W) = -0.5 \tag{4}$$

The value returned by $value(e)$ represents the contribution of event e to the involved node's reputation. Forwarding completion events are positive (therefore, positive values are returned), while the other three event types are negative. Thus, the returned value can be viewed as a positive event count. Since warning events contain indirect reputation information provided by other nodes, this type of event contributes less to reputation calculations compared to other event types. Accordingly, the returned value of a warning event is set to -0.5. A weight function for increasing the contribution of more recent events to reputation value can be defined as

$$weight(i) = \frac{\alpha * (1-\alpha)^i}{\sum_{j=1}^{K} \alpha * (1-\alpha)^j} \tag{5}$$

where α is a system parameter with values ranging from 0 to 1. Equation (5) has two important features: (a) for any value of K, the sum of $weight(1)$ to $weight(K)$ is 1, and (b) the value of $weight(i)$ decreases with an increase of i.

Let r_n be the reputation value of node n. r_n is calculated as

$$r_n = \sum_{i=1}^{K} weight(i) * value(e_i) \tag{6}$$

Equation (6) gives more weight to new rather than old events. Figure 1 shows the weights assigned to each event given $K = 10$, and Figure 2 shows cumulative weight values for various quantities of recent events. According to Equations (5) and (6), reputation values are between -1 and 1.

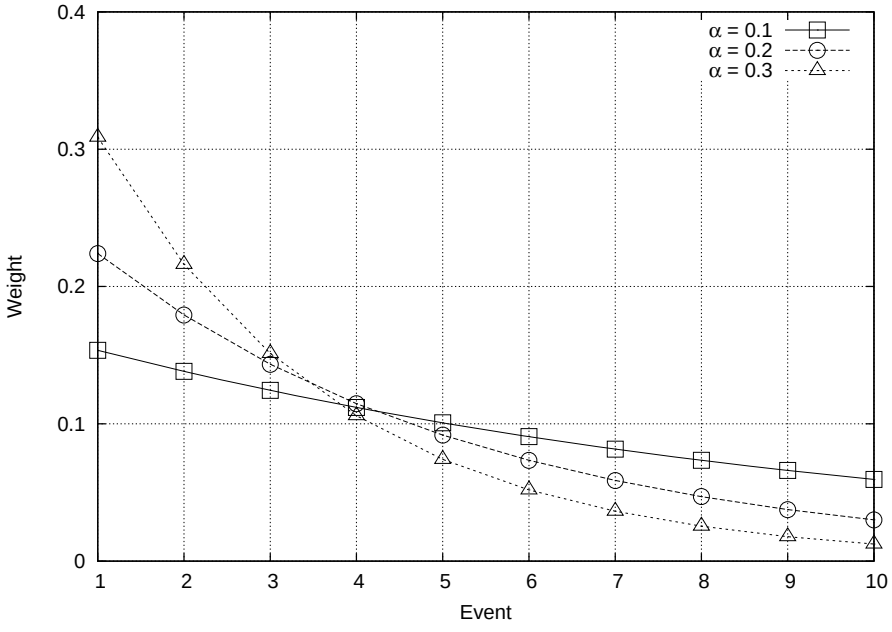

FIGURE 1. Weight assignments for individual events

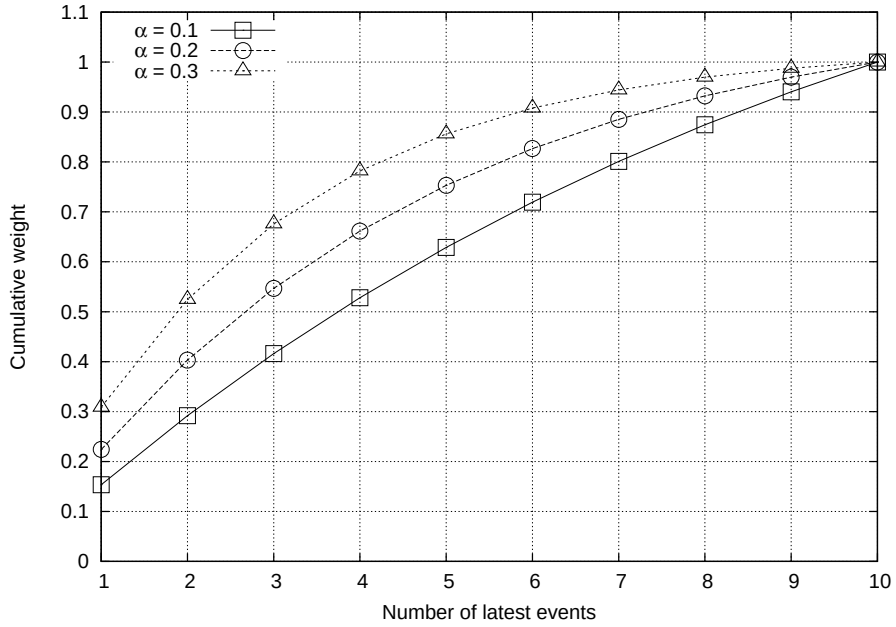

FIGURE 2. Cumulative weights plotted against numbers of most recent events

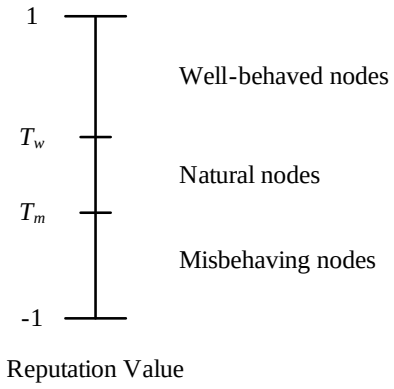

FIGURE 3. Node categories

3.3. **Forwarding node selection.** Let T_w and T_m be two thresholds. After calculating the reputation values of neighboring nodes, those nodes are classified as (a) well-behaved (values exceeding T_w); (b) misbehaving (values below T_m); or (c) natural (values between T_m and T_w) (Figure 3). According to the functions of T_m and T_w, both thresholds exist between -1 and 1. In addition, T_w is larger than T_m. Nodes that want to transmit packets initially select adjacent and well-behaved nodes with the shortest distances to their destinations. If none exist, nodes classified as natural are inspected next, and nodes classified as misbehaving are checked last. Since forwarding nodes are selected according to geographic position and reputation value, packet delivery ratios can be increased by reducing the potential for being dropped by misbehaving nodes.

According to these rules, T_m exerts greater impact than T_w on the selection process for forwarding nodes. Nodes with reputation values below T_m are the last to be selected, while T_w exerts little impact on forwarding node selection. To give an example, assume that T_w is set to a large value such as 0.9. If no nodes have reputation values less than 0.9, natural nodes will be selected – in other words, T_m should be set at a value close to

0 in order to isolate misbehaving nodes. If T_m is set to a value close to -1, most nodes will be either well-behaved or natural. Since forwarding node selection is based on node category, there is greater likelihood for a misbehaving node to be selected as a forwarding node, resulting in a low packet delivery ratio.

4. Experiments and Discussion.

4.1. **Setup.** A test of our proposed reputation management tool was conducted using ns-2 [24] – the most frequently used one in wireless ad hoc network environments, and one that provides some of the latest communication modules. Vehicular movement traces were generated with VanetMobiSim [25]. Unless otherwise noted, the parameter values in Table 1 were used in all experiments. To avoid large communication overhead, the transmission range of warning messages was set to 500 meters. T_w, T_m, α, and K were set to values believed to maximize performance. Figure 4 shows the road topology used for evaluation purposes. A total of six vehicular movement traces were generated, with five simulation tasks performed for each one. Ten connections were established for each simulation task.

TABLE 1. Simulation parameter settings

Parameter	Value
Network simulator	ns-2 v2.34
Map area	3,000 m $*$ 3,000 m
MAC protocol	IEEE 802.11p
Radio transmission range	300 m
Traffic type	CBR (UDP)
Number of connections	10
Packet size	512 bytes
Vehicle density	30 cars/km^2
Vehicle speed	8.33-13.89 m/second
Simulation time	900 seconds
Warning packet transmission range	500 m

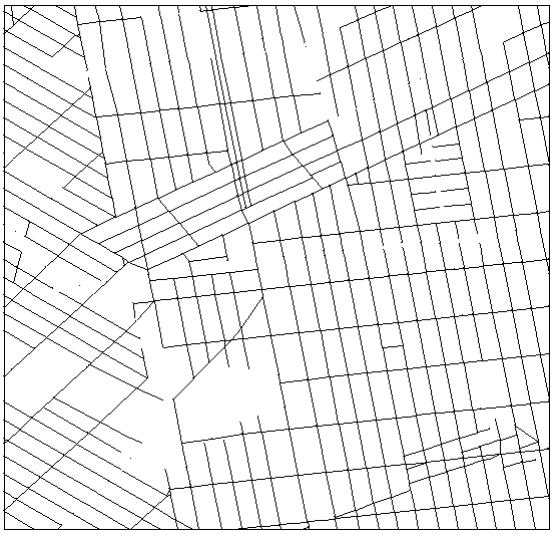

FIGURE 4. Simulation map

4.2. **Results and analysis.** We analyzed relationships among parameter settings, PDRs, and communication overhead for our proposed system. PDR is defined as the number of packets received by destination nodes divided by the number of packets transmitted by source nodes. Data for the effects of different warning message transmission ranges on PDR are shown in Figure 5. The results indicate that for a given misbehaving vehicle percentage, warning message range variability exerted little impact on PDR. When the warning message range was set to 500 meters, warning messages could reach not only all neighboring nodes, but also non-neighboring nodes within 500 meters via neighbor node forwarding. Accordingly, warning message ranges greater than 500 meters did not cause significant PDR improvement, but incurred significantly greater communication overhead. Figure 6 shows the additional communication overhead generated by our proposed system compared to the T-GPSR protocol. At a warning message range of 500 meters, our proposed system generated marginally greater communication overhead (less than 5%). Communication overhead for a message range of 1,000 meters was nearly twice that for a range of 500 meters. The increase between 1,000 and 1,500 meters was less significant because of the size of the simulation map used in our experiments (3,000 m $*$ 3,000 m). At a range of 1,500 meters, the coverage area for some vehicles could have exceeded the map boundaries, depending on placement. Warning message coverage areas were much smaller for vehicles located near map margins. We believe that larger maps would generate much greater communication overhead for warning message ranges between 1,500 and 2,000 meters. As shown in Figures 5 and 6, warning message transmission ranges for our proposed system could be set to values roughly twice the radio transmission range, yet still achieve good PDR performance with low communication overhead.

Figures 7 through 9 present data on relationships between PDR and misbehaving vehicle percentages for different α and T_m values. For any given value of α, PDR decreased as T_m decreased. The reason is that a lower T_m value increased the time required for a node to identify misbehaving nodes, resulting in a larger number of packets being dropped. For any given value of T_m, α exerted a smaller impact on PDR than T_m plus a fixed value of

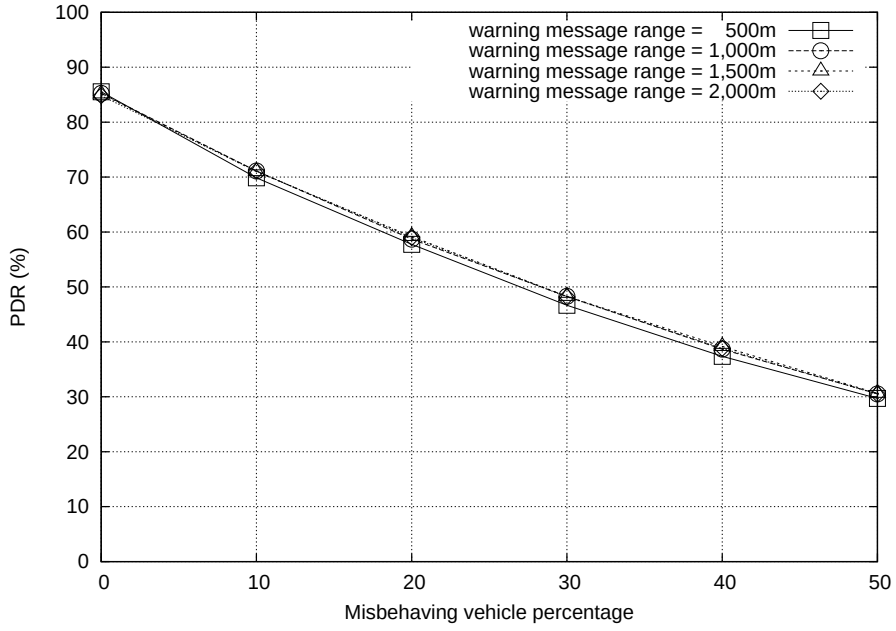

FIGURE 5. Packet delivery ratios (PDRs) plotted against misbehaving vehicle percentages for different warning message ranges

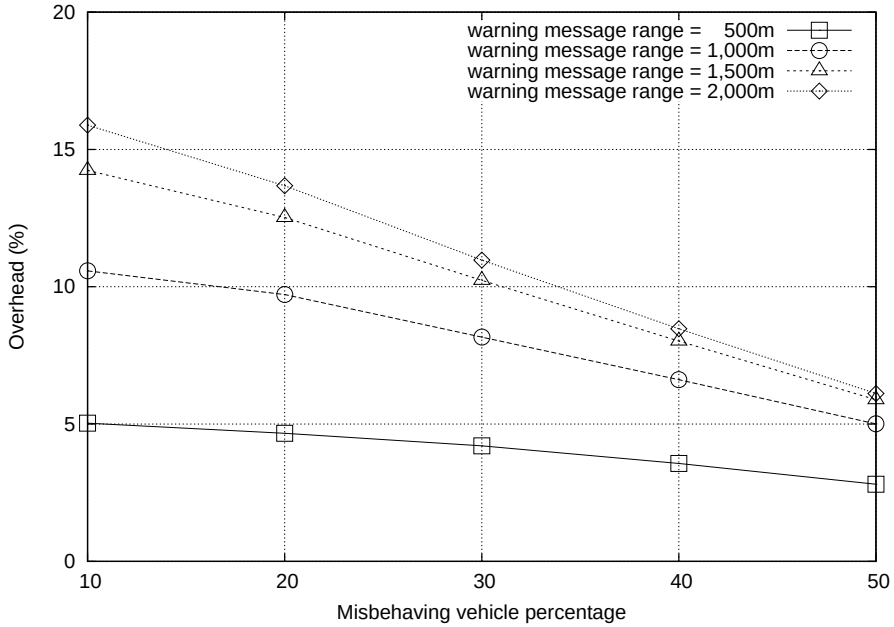

FIGURE 6. Extra communication overhead values plotted against misbehaving vehicle percentages for different warning message ranges

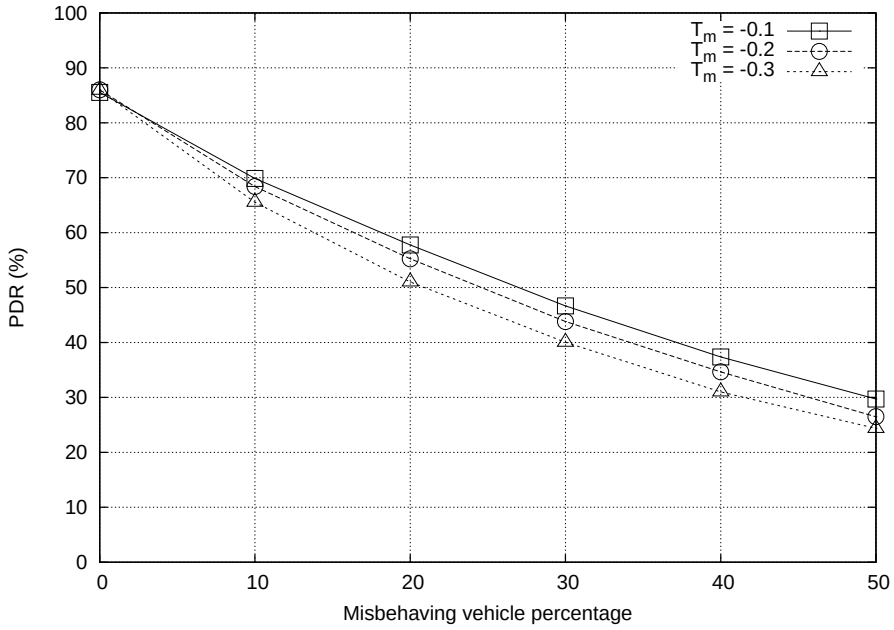

FIGURE 7. Packet delivery ratios (PDRs) plotted against misbehaving vehicle percentages ($\alpha = 0.1$)

α. As stated earlier, α determines the weights of the most recent events when calculating node reputation values. A large α results in a significant variance in reputation value based on a single event. Accordingly, a large T_m (e.g., -0.1) and a small α (e.g., 0.1) are preferable for our proposed system.

Results for the effects of various misbehaving vehicle percentages on PDR are shown in Figure 10. Our proposed method produced higher PDR values compared to the GPSR and T-GPSR methods. When the network in question had 0% misbehaving vehicles,

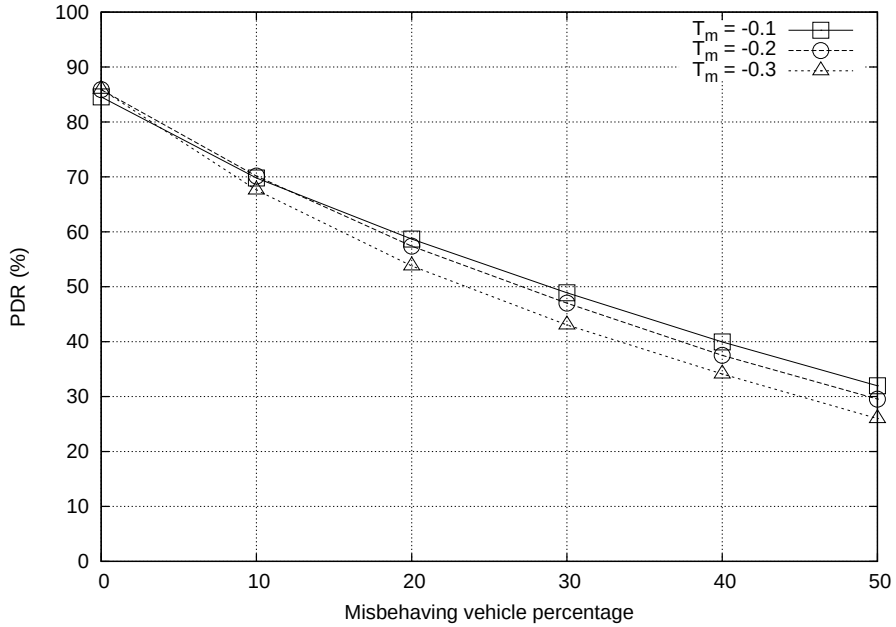

FIGURE 8. Packet delivery ratios (PDRs) plotted against misbehaving vehicle percentages ($\alpha = 0.2$)

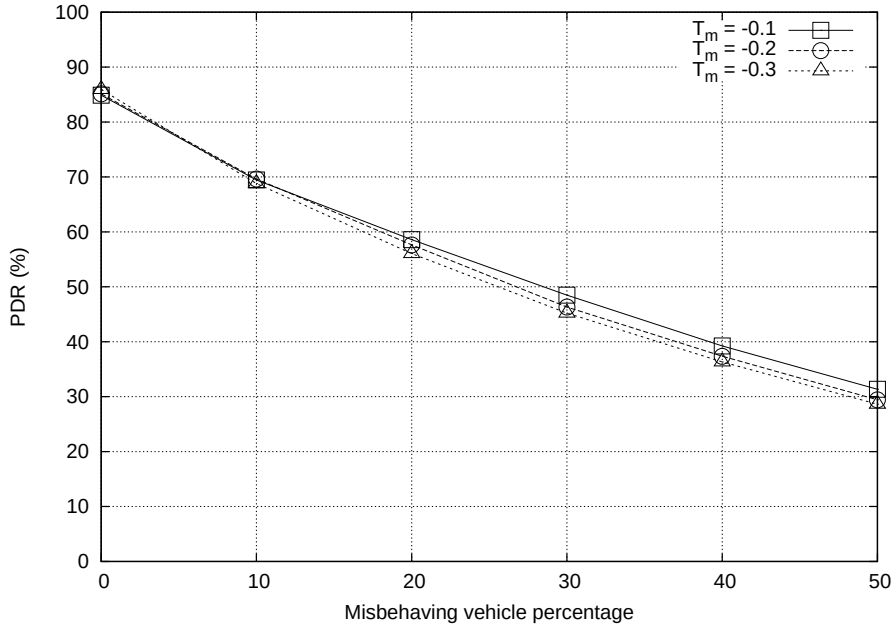

FIGURE 9. Packet delivery ratios (PDRs) plotted against misbehaving vehicle percentages ($\alpha = 0.3$)

all methods achieved identical PDR values. However, when the misbehaving vehicle percentage increased to 10%, our method produced an 8% larger PDR value compared to the T-GPSR method, and 16% larger than the GPSR method. PDR improvement was further enhanced by our method when the percentage increased to 20%. A likely explanation is that at 10% it was easier for other methods to select non-misbehaving vehicles when reputation was not considered, but it was more difficult to do so at 20%, resulting in more packets being dropped by misbehaving vehicles (Figure 11). PDR

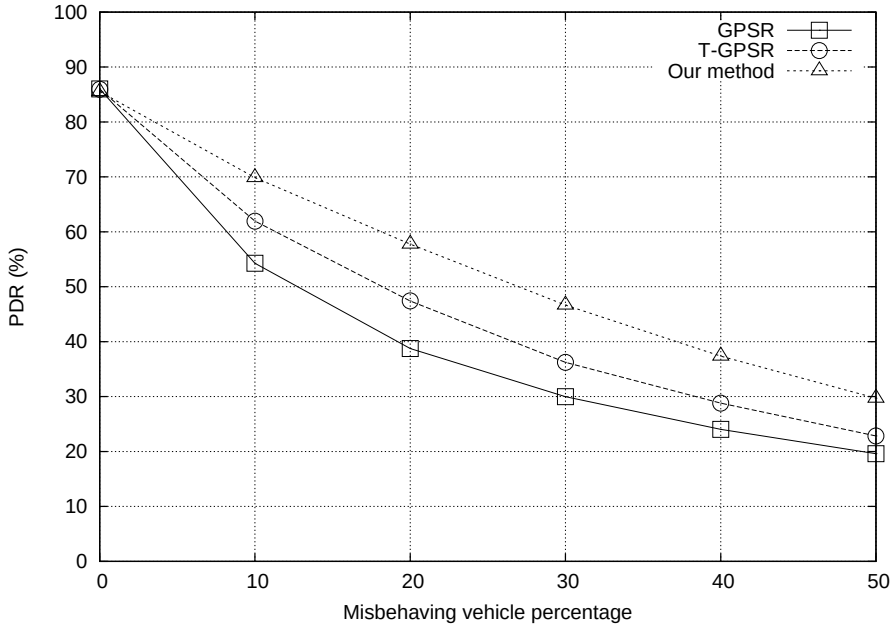

FIGURE 10. Packet delivery ratios (PDRs) plotted against misbehaving vehicle percentages for different methods

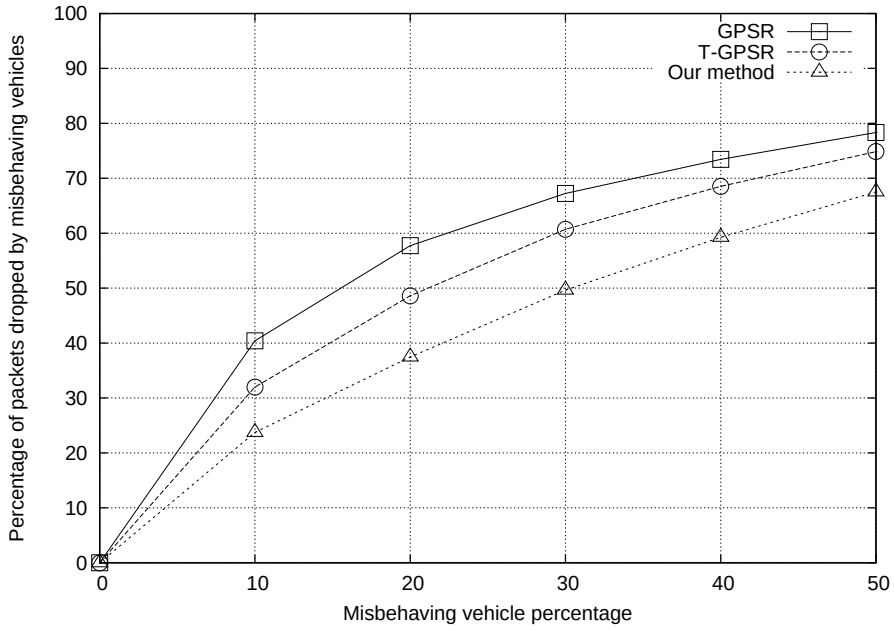

FIGURE 11. Percentages of packets dropped by misbehaving vehicles plotted against misbehaving vehicle percentages for different methods

improvement for our method started to decline at a misbehaving vehicle percentage of 30% or more, since it was difficult for vehicles to find adjacent vehicles that were well-behaved. In short, the GPSR had the lowest PDR compared to the other two methods because it did not consider reputation when selecting forwarding nodes. Since our proposed method was capable of detecting misbehaving nodes more quickly and precisely, it achieved higher PDR values than the T-GPSR method. Further, the number of packets dropped by

misbehaving nodes in our proposed method was smaller than the numbers dropped by the GPSR and T-GPSR methods.

5. **Conclusion.** VANET success is strongly dependent on all vehicles sharing information via reliable transmission routes. In this paper we described our proposal for a distributed reputation management system for identifying misbehaving vehicles – that is, vehicles that refuse to forward messages, or that somehow modify forwarded messages. Our system uses a forwarding node selection process to exclude misbehaving vehicles, thereby resulting in higher packet delivery ratios compared to existing methods. Compared to T-GPSR, our proposed system incurred a small amount of communication overhead by limiting the size of the control packet broadcast area.

We see two possible directions for extending this work. The first involves the transmission range of warning messages, which was fixed for the present project. Since reductions in transmission range in high vehicle density areas would lower the amount of communication overhead resulting from warning messages, the impacts of variation in transmission ranges on packet delivery ratio require further study. Second, in our method a node calculates the reputation values of other nodes based on a combination of its own observations and warning messages sent by others. It is important to remember that misbehaving nodes have some potential to send fake warning messages that can cause network damage; therefore, a cheat-proof mechanism in the reputation management system is required to mitigate the negative effects of false warnings.

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

[1] S. K. Bhoi and P. M. Khilar, Vehicular communication: A survey, *IET Networks*, vol.3, pp.204-217, 2014.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin and T. Weil, Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions, *IEEE Communications Surveys & Tutorials*, vol.13, pp.584-616, 2011.

[3] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti and H. Zedan, A comprehensive survey on vehicular ad hoc network, *Journal of Network and Computer Applications*, vol.37, pp.380-392, 2014.

[4] R. D. Pietro, S. Guarino, N. V. Verde and J. Domingo-Ferrer, Security in wireless ad-hoc networks – A survey, *Computer Communications*, vol.51, pp.1-20, 2014.

[5] M. N. Mejri, J. Ben-Othman and M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions, *Vehicular Communications*, vol.1, pp.53-66, 2014.

[6] R. G. Engoulou, M. Bellaiche, S. Pierre and A. Quintero, VANET security surveys, *Computer Communications*, vol.44, pp.1-13, 2014.

[7] N. J. Patel and R. H. Jhaveri, Trust based approaches for secure routing in VANET: A survey, *Procedia Computer Science*, vol.45, pp.592-601, 2015.

[8] A. Dahiya and R. K. Chauhan, A comparative study of MANET and VANET environment, *Journal of Computing*, vol.2, pp.87-92, 2010.

[9] J. Zhang, A survey on trust management for VANETs, *Proc. of IEEE International Conference on Advanced Information Networking and Applications*, Biopolis, Singapore, pp.105-112, 2011.

[10] T. Thenmozhi and R. M. Somasundaram, Towards modelling a trusted and secured centralized reputation system for VANETs, *Wireless Personal Communications*, vol.88, pp.357-370, 2016.

[11] X. Zhuo, J. Hao, D. Liu, and Y. Dai, Removal of misbehaving insiders in anonymous VANETs, *Proc. of the 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Tenerife, Canary Islands, Spain, pp.106-115, 2009.

[12] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J.-P. Hubaux, Eviction of misbehaving and faulty nodes in vehicular networks, *IEEE Journal on Selected Areas in Communications*, vol.25, pp.1557-1568, 2007.
[13] M. Raya, P. Papadimitratos, V. D. Gligor and J.-P. Hubaux, On data-centric trust establishment in ephemeral ad hoc networks, *Proc. of the 27th IEEE Conference on Computer Communications*, Phoenix, Arizona, USA, pp.1912-1920, 2008.
[14] B. Ostermaier, F. Dotzer and M. Strassberger, Enhancing the security of local danger warnings in VANETs – A simulative analysis of voting schemes, *Proc. of the 2nd International Conference on Availability, Reliability and Security*, Vienna, Austria, pp.422-431, 2007.
[15] J. Wang, Y. Zhang, Y. Wang and X. Gu, RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enable VANETs, *International Journal of Distributed Sensor Networks*, vol.12, 2016.
[16] S. Marti, T. J. Giuli, K. Lai and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, *Proc. of the 6th Annual International Conference on Mobile Computing and Networking*, Boston, Massachusetts, USA, pp.255-265, 2000.
[17] S. Buchegger and J. Y. Le Boudec, Performance analysis of the CONFIDANT protocol, *Proc. of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Lausanne, Switzerland, pp.226-236, 2002.
[18] P. Michiardi and R. Molva, CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, *Advanced Communications and Multimedia Security*, pp.107-121, 2002.
[19] D. B. Johnson and D. A. Maltz, Dynamic source routing in ad hoc wireless networks, *Mobile Computing*, pp.153-181, 1996.
[20] C. Perkins, E. Belding-Royer and S. Das, Ad hoc on-demand distance vector (AODV) routing, *RFC 3561*, 2003.
[21] B. Karp and H. T. Kung, GPSR: Greedy perimeter stateless routing for wireless networks, *Proc. of the 6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, USA, pp.243-254, 2000.
[22] A. A. Pirzada and C. Mcdonald, Trusted greedy perimeter stateless routing, *Proc. of the 15th IEEE International Conference on Networks*, Adelaide, Australia, pp.206-211, 2007.
[23] A. A. Pirzada and C. McDonald, Establishing trust in pure ad-hoc networks, *Proc. of the 27th Australasian Conference on Computer Science*, Dunedin, New Zealand, pp.47-54, 2004.
[24] *The Network Simulator*, http://www.isi.edu/nsnam/ns/.
[25] *VanetMobiSim*, http://vanet.eurecom.fr/.