Stimulating Cooperation in Vehicular Ad Hoc Networks: A Coalitional Game Theoretic Approach

Tingting Chen[1] Liehuang Zhu[2] Fan Wu[3] Sheng Zhong[1]
1 Computer Science and Engineering Department, SUNY Buffalo
{tchen9, szhong}@buffalo.edu
2 Computer Science and Engineering Department, Beijing Institute of Technology
liehuangz@bit.edu.cn
3 Department of Computer Science and Engineering, Shanghai Jiao Tong University
fwu@cs.sjtu.edu.cn

***Abstract*—In Vehicular Ad Hoc Networks (VANETs), because of the non-existence of end-to-end connections, it is essential that nodes take advantage of connection opportunities to forward messages, to make end-to-end messaging possible. Thus it is crucial to make sure that nodes have incentives to forward messages for others, despite that the routing protocols in VANETs are different from traditional end-to-end routing protocols. In this paper, we study how to stimulate message forwarding in VANETs. Our approach is based on coalitional game theory. In particular, we propose an incentive scheme for VANETs and rigorously show that with our scheme faithfully following the routing protocol is to the best interests of each node. In addition, we extend our scheme to take the limited storage space of each node into consideration. Experiments on testbed trace data verify that our scheme is effective in stimulating cooperation of message forwarding in VANETs.**

I. Introduction

Vehicular ad hoc networks support communications among smart vehicles, and between vehicles and nearby roadside equipment. There can be numerous useful and interesting services on the road provided by VANETs [1], [2], [3], [4], [5], [6] in the near future. In VANETs, effective and efficient message delivery among vehicles must be guaranteed. Under some circumstances, (e.g., night-time with low vehicular density, or disseminating commercial ads through VANETs), to overcome the difficulty of intermittent connectivity, store-carry-and-forward message switching becomes an important idea of routing in VANETs. A node stores and carries messages; it considers forwarding a message to another node whenever these two nodes come into the communication range of each other. In this way, each message is forwarded from one node to another. A number of routing protocols (e.g. [7], [8], [9], [10], [11]) have been proposed to increase the likelihood of successfully delivering a message, which can be applied to VANETs.

However, even if we have a good routing protocol for a VANET, it is still a crucial question whether nodes will *follow the protocol or not*. The necessity of solving this problem can been observed in the perspectives of two types of nodes. On the one hand, an ordinary node of the VANET may belong to an individual user and thus be *selfish*. It may be unwilling to forward messages of others for nothing, and moreover carrying message takes its own storage space. On the other hand, in many routing protocols, nodes with special abilities, (e.g. those with more active mobility on the road, like Taxi cars), are more likely to be picked as forwarders. For these nodes, the situation is worse: even though they are willing to forward messages initially, the overwhelming load of services for others will soon consume so much of their communication resource (e.g., wireless bandwidth and storage space) that they have to deviate from the protocol to save their own resource. Therefore, it is highly important to give nodes incentives, stimulating them to cooperate in forwarding messages.

Indeed, automotive industry controls the vehicle manufacture. However, we can also foresee some problems of cooperation even if the manufacturers do not leave it as an option for the users to choose being cooperative or not. Actually, after the vehicles are sold, they are under the full control of the users. Thus, although the manufacturer does not leave an option for the users to choose being cooperative or selfish, the users can still get help from some expert hackers in changing the VANETs protocols running in the vehicles, so that they can be 'free riders' in the network without contributing anything. Hence, we believe that mandatory cooperation in VANETs is difficult to achieve and designing incentive-compatible packet forwarding protocols can help providing a feasible way to enforce the mandatory cooperation in VANETs.

There are two types of existing incentive mechanisms for stimulating cooperation in wireless networks: reputation-based approaches (e.g., [12], [13], [14]) and credit-based approaches (e.g., [15], [16]). Reputation-based approaches rely on observ-

Correspondence Author: Sheng Zhong, Department of Computer Science and Engineering, State University of New York at Buffalo, Amherst, NY 14260, U. S. A. Phone: +1-716-645-4752. Fax: +1-716-645-3464. Email: szhong@buffalo.edu

This paper was partly done while Fan Wu was a student at SUNY Buffalo.
This work was supported by NSF CCF-0915374 and NSF CNS-0845149.

ing the behavior of neighbor nodes and punishing the detected uncooperative nodes to stimulate cooperation. In VANETs, however, for a distributed reputation system, the deviating behaviors of a selfish node are more difficult to be observed and determined by other nodes, because the connections with the same nodes are occasional. A recent work on incentive aware routing in delay tolerant networks[17] cannot be applied to VANETs for a similar reason: The authors use tit-for-tat mechanism in which nodes reward or punish their neighbors based on the history they have observed; however, in VANETs, the connection opportunity between any two nodes may only be once and thus the neighborhood relationship cannot easily be established. Of course, if a centralized reputation controller is established in the VANET, it could collect and broadcast the reputation of any node to help stimulate the cooperation in the network. In this paper, we aim at another approach, credit-based mechanisms, to encourage cooperation by rewarding credits to the cooperative nodes. This idea is especially appropriate for many applications in VANETs, such as disseminating advertisement using vehicles. In existing works for traditional multi-hop networks, the credit-based mechanisms depend on end-to-end connections to determine how many credits each node should receive. In VANETs, since end-to-end paths are not guaranteed at all, existing credit-based mechanisms cannot be used either.

In this paper, we use an approach based on *coalitional game theory* to solve the *forwarding cooperation problem in VANETs*. In particular, we say a node is cooperative in forwarding in VANETs, if it follows the routing protocol. In a coalitional game, there are a number of players. These players correspond to the nodes in a VANET. When the players in a subset decide to cooperate within the subset, the subset is called a *coalition*. In particular, the coalition of all players is called the *grand coalition*. Hence, our goal is to ensure that, whenever a message needs to be forwarded in a VANET, all involved nodes have incentives to form a grand coalition. In coalitional game theory, there is a strong solution concept, namely *core*, that can provide such guarantees.

We propose an incentive scheme for VANETs and rigorously analyze it in the framework of coalitional games, showing that, when it is used, following the protocol is in the core of the coalitional game. In addition, we extend our scheme to take the limited storage space of each node into consideration. When a node does not have sufficient space for storage, it has to discard some of the messages. To decide which messages to discard, a lot of routing protocols (e.g., [10], [6], [18]) require some auxiliary information to be transmitted in control messages, such as the probabilities of meeting the destinations. Although in principle we can stimulate the forwarding of these control messages using the same method that we use for data messages, it would require lots of overheads to do so. To make our scheme more efficient, we propose a light-weight approach which makes full use of the selfishness of the autonomous nodes, giving them the freedom to choose which messages to discard. Our extended scheme guarantees that it is to the best interest of each node to discard the messages that the system prefers to drop.

There are a few existing works [19], [20] on the incentive problems of packet forwarding in VANETs. However, they either target a specific routing goal (e.g., [19]), or does not have a rigorous proof for nodes' cooperation (e.g., [20]). In contrast, our work considers the incentives for all nodes including the sources and guarantees the cooperation of them under rigorous theoretical analysis. For a more detailed comparison, please see Section II.

The rest of the paper is organized as follows. Section II, presents brief reviews of the related works. In Section III we introduce basic concepts in coalitional game theory, and present a model of the forwarding cooperation problem in VANETs. Section IV describes the incentive scheme. In Section V, an extension to limited storage space is considered. Experimental evaluation results are presented in Section VI. We conclude our paper in Section VII.

II. Related Work

A number of DTN routing protocols have been proposed, which can be applied to VANETs. They can be roughly classified into two categories based on the strategies that they use, flooding (replication) based protocols (e.g., [9], [11], [10], [6]) and forwarding based protocols (e.g., [21], [8], [7]). Flooding based protocols allow to make message replications in order to increase the probability for any copy of the message to reach destination. For example, in epidemic routing [9], if a node has a message to send, it transmits the copies to all the nodes it meets in the random movement. The Spray-and-Wait routing [21] also falls into this category. In contrast, a lot of works focus on forwarding strategies using knowledge about the network without flooding. The forwarding strategy based protocols rely on knowledge about the network to select the best path to the destination. Recently, in [18] a routing protocol is proposed to intentionally optimize one chosen performance metric. However, all these works have not considered the incentives of nodes to cooperate, which may lead to performance degradation in face of selfish nodes.

The incentive mechanisms for routing in wireless networks can be broadly divided into two categories: reputation systems (e.g., [12], [13], [14], [22]) and credit-based systems (e.g., [15], [16], [23], [24], [25], [26], [27]). Game theory has been extensively applied to design and analyze such incentive mechanisms. For example, in [22], a reputation mechanism is modeled as a repeated reputation game and the analysis of the game helps to assess the robustness of the reputation scheme. Different from our paper, their work does not use micropayment to stimulate the cooperation. Instead, nodes in the network can punish each other if they have observed the selfish behavior of the cheaters, by refusing to forward packets for them. In contrast, in credit-based systems such as [15], [16], [26], [27], pricing schemes are often leveraged in order to enforce nodes collaboration, and micropayment is used to implement the pricing schemes. For example, in [26], a practical incentive scheme based on micropayment is proposed for traditional multi-hop wireless networks. The major difference of this work and ours is that we separate the behavior of receiving and forwarding the message in the payment scheme. This is due to the fact that under many

circumstances of VANETs, the connectivity between nodes is intermittent and thus there is good chance that messages received are lost before meeting the subsequent node (which is not the case for traditional multi-hop wireless networks). In summary, all of the existing schemes are designed for traditional end-to-end routing systems only. Since VANETs are fundamentally different from traditional end-to-end routing systems, it is very difficult to apply these works VANETs.

In inter-vehicle communication, Public Key Infrastructure (PKI) has become the most suitable security building block for VANETs to satisfy security requirements [28], [29]. Digital signatures can be processed using computing resources equipped in vehicles[30]. In our scheme, we also utilize a public key infrastructure as a building block, to verify the identities of vehicles through wireless connections. Usually in VANETs, for security reasons identity verification is required for the message sender. In our scheme when a node wants to forward message to the subsequent node, certified identities are needed both for the subsequent node and the message forwarder.

In [19], a secure incentive framework is presented for commercial ad dissemination in VANETs. Commercial ad dissemination has a specific routing goal, (namely, sending the ad message to as many nodes as possible). Their solution is designed for this goal, and thus does not apply to packets that have only one or some destinations. Li and Wu [20] proposed a nice incentive scheme that solved the overspending problem for VANETs. They use a forwarding tree to represent the message propagation process and allocate weighted rewards to the intermediate nodes according to their positions in the forwarding tree. Our scheme also considers the incentive of the source node, but it has a major difference from the scheme in [20]. Our scheme has rigorous analysis of incentives while the scheme in [20] does not.

Recently in [31], Wu et. al. propose an incentive compatible opportunistic routing scheme. Their focus is on making sure the nodes to faithfully follow the protocol (i.e., reporting link loss and so on) in the process of making routing decisions, while our objective is to enforce the nodes to cooperatively forward the packets as required by the routing decisions. So the solutions in [31] can not be applied to solve the problem in this paper.

III. System Model

In this section, first we briefly review some basic concepts in coalitional game theory that will be needed in our analysis. Then we present a coalitional game model for message forwarding in VANETs.

A. Coalitional Game and The Core

In coalitional game theory, the central concept is the formation of coalitions. Each coalition is a subset of game players who cooperatively join their forces. Each selfish player always tries to join the coalition that can maximize its own payoff share. Denote by $\mathbf{R}$ the set of real numbers. Formally, a coalitional game can be defined as follows.

Definition 1: A coalitional game is an ordered pair ($\mathbf{N}$, v), where $\mathbf{N}$ is the set of players and v is a characteristic function from $2^{\mathbf{N}}$ to $\mathbf{R}$ such that $v(\phi) = 0$. Each subset of $\mathbf{N}$ is called a coalition. Hence, the characteristic function v actually assigns a real number to each coalition, called the payoff of that coalition. The coalition $\mathbf{N}$, which consists of all players, is called a grand coalition.

Intuitively, for a coalition S, $v(S)$ is the amount of overall benefit that can be obtained by the players in S from cooperation agreements among them.

Ideally, all players join the grand coalition so that any two players cooperate with each other. Since each player has the freedom to choose the coalition to join based on its own interests, we must ensure that joining the grand coalition is to the best interest of every player. In coalitional game theory, there is a classic solution concept, *core*, which gives us such a guarantee.

Definition 2: In a coalitional game $(\mathbf{N}, v)$, the core $C(v)$ is the set of payoff allocation vectors $x \in \mathbf{R}^{\mathbf{N}}$, s.t.

$$C(v) = \{x \in \mathbf{R}^{\mathbf{N}} | \sum_{i \in \mathbf{N}} x_i = v(\mathbf{N}); \sum_{i \in S} x_i \geq v(S), \forall S \subseteq \mathbf{N}\},$$

where x_i is the payoff allocation to player i.

From the above definition we can see that an allocation lies in the core is *efficient* [32] in that $\sum_{i \in N} x_i = v(\mathbf{N})$, which means no payoff is wasted. Moreover, because $x_i \geq v(\{i\})$, an allocation in the core is *individually rational* [32], which means each player can obtain a payoff share no less than acting alone. (In fact, each player's payoff share is no less than joining any other coalition.)

Note that the core of a coalitional game may be of any size; it may even be empty. If the core is empty, then it is cannot guaranteed that it is to the best interest of every player to join the grand coalition.

B. Coalitional Game Formation in VANETs Message Forwarding

In this subsection, we introduce the VANET system model used in this paper and present a coalitional game model for message forwarding in VANETs.

We consider a VANET with a set of mobile nodes. Two nodes can exchange messages when they are within the transmission range of each other. Here we consider a general routing protocol, denoted by $\Re$. Note that $\Re$ could be one of the many existing routing protocols. In this paper, we assume that there is only one routing protocol in the system. It is a very interesting problem when there are different routing protocols coexisting in the network. If each node knows which routing protocol should be chosen, our incentive scheme can be extended to cope with this situation by adding one more piece of information into the message receipt, indicating the routing protocol used for the message transmission. Otherwise, we will have a new challenging problem; We leave it to future study.

In the VANET, messages can be delivered directly to the destination or forwarded by some intermediate nodes before reaching destination. The intermediate node may or may

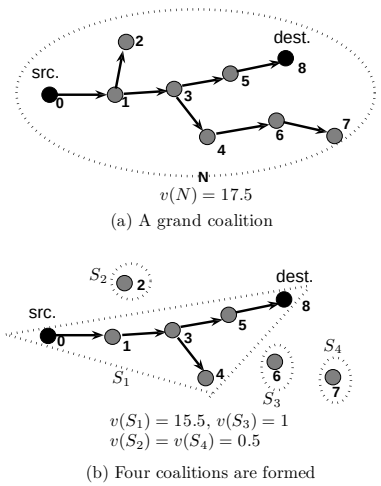
not replicate a copy of the message and keep it during the transmission, according to different routing protocols. Note that in this paper we use the term, *forwarding*, in a very general sense; by forwarding a message we mean either the transfer of the message itself or the transfer of its copies to the next hop.

A directed graph $G = (V, E)$ is used to describe the forwarding of each message. V is the set of nodes that are required to participate in routing this message by $\Re$. Each directed edge in E represents that the message is forwarded from the tail node to the head node. In other words, the graph G records the traces of a message and its copies. In some application scenarios, nodes are all equipped with GPS. Then it is possible to modify the V to create geo-referenced coalitional games. In particular, using geo-location information, we can only consider the nodes that meaningful with respect to source and destination, so that the signaling and communication overhead can be reduced. Here in our game, to keep it general, the nodes are those who are required to forward packets by the routing protocol.

We now model the transfer of a message from its source ($src.$) to its destination ($dest.$) as a forwarding coalitional game. The forwarding coalitional game $(\mathbf{N}, v)$ starts when the message is generated by $src.$, and ends after it and its copies disappear in the network, either successfully received by the $dest.$ or discarded by all intermediate nodes in halfway. The players are the nodes in V (i.e. $\mathbf{N} = V$), including $src.$ and $dest.$. In the process of this message being transferred from one node to another, two nodes are in a coalition, if the message (or its copy) is transmitted between them in the way defined in $\Re$. We call the forwarding behaviors specified by $\Re$, legal forwarding, for convenience in the rest of this paper. The coalitional relationship is *transitive*, i.e. if node p and q are in a coalition, and meanwhile q and r are in a coalition, then p and r are in the same coalition.

Recall that to form the forwarding coalitional game $(\mathbf{N}, v)$, $\mathbf{N}$ and v must be specified. Since in VANETs the end-to-end connections are not guaranteed, the first challenge to form the forwarding coalitional game, is to determine the nodes that should be involved the message forwarding according to $\Re$, i.e. players set $\mathbf{N}$. The difficulty lies in the fact that in VANETs routing protocols, the next forwarder can only be determined when the carrier and the potential forwarder actually meet based on some routing information (In this paper, by *meet* we mean two nodes come in the communication range with each other.). To clarify the $\mathbf{N}$ for each game, we use a stimulating approach to encourage the nodes to report their meetings. Every time two nodes meet, each node keeps a brief record of their meeting and the routing information. For reporting each record, nodes (except $src.$) can obtain an amount of reward, u, for assisting to determine the player set $\mathbf{N}$. We note that the reason of keeping records of neighbors is for enforcing the incentive scheme, not for routing messages in the VANETs. Our incentive scheme can work with routing protocols that do not need the information about neighbors. We will present the specific system design, e.g., where and how the records will be reported and content of the record in detail in Section IV.

An important component in a coalitional game is the definition of the payoff (worth) of a coalition S, $v(S)$. Naturally, the total payoff of a coalition should reflect their success in forwarding the message to $dest.$. Let $d(S)$ denote the number of message copies that are successfully delivered to $dest.$ within coalition S. We can formulate the worth of coalition S as follows.



(a) A grand coalition

(b) Four coalitions are formed

Fig. 1. Illustration of forwarding coalitional game model.

$$v(S) = \delta \cdot d(S) + u \cdot n_{rec}(S), \tag{1}$$

where δ is a system parameter representing the reward for successfully delivering one message copy,[1] and u is the unit amount of reward for reporting a record. $n_{rec}(S)$ is the number of meeting records submitted by the members in S. In words, the worth of a coalition consists of two parts, rewards for successfully transferring data to $dest.$, and rewards for helping determine the player set $\mathbf{N}$. Clearly, if $dest.$ is not in S, then $d(S) = 0$. Moreover, by the transitivity of the coalition, $d(S) > 0$ if and only if both $src.$ and $dest.$ are in S.

In Figure 1, we illustrate the forwarding coalitional game model with two examples. Their description graphs G are in subfigures (a) and (b) respectively. The locations of the nodes in the graph have no physical meaning. The number labeling each node is the node ID. Recall that each edge represents a legal forwarding between the two nodes. In subfigure (a), all players form a grand coalition $\mathbf{N}$, that is, all players involved in the transmission follow the routing protocol $\Re$. In (b), the legal forwarding between nodes 1 and 2 does not happen when the two nodes meet; neither do those between 4 and 6, 6 and 7. As a result, in the forwarding coalitional game, 4 coalitions are formed. In the two games, all nodes report their meeting records, for the rewards. Let $\delta = 10$ and $u = 0.5$. For the grand coalition, $d(N) = 1$, and $n_{rec}(N) = 15$ (because each meeting is reported twice by the nodes excluding the source), then according to Eq. (1) $v(N) = 17.5$. In Figure

[1]From the source and the destination's point of view, it suffices to have a single copy transferred to the destination, and so it seems unnecessary to reward the transfer of each copy of the message. Nevertheless, since each copy of message is typically transferred by different nodes, if we don't reward the transfer of every copy, the result could be that no copy of the message is transferred.

1(b), $d(S_1) = 1$, but $d(S_2) = d(S_3) = d(S_4) = 0$ because the destination is not included in S_2, S_3, S_4. Similarly, according to Eq. (1) we can calculate the worth of each coalition in each game as shown in the figure.

IV. Incentive Scheme for VANETs Message Forwarding

After establishing the forwarding coalitional game model, in this section we design an incentive scheme for VANETs message forwarding based on this model. First, we present the system architecture and we introduce a payoff allocation method that we will use in the incentive scheme. Then, we rigorously show that it can result in a strongly stable state which is in the core. After that, we present a complete design of our incentive scheme based on our payoff allocation method. Finally, we describe how our scheme deals with cheating.

A. System Architecture

The overall architecture of the system consists of a number of smart vehicles that have VANET communication devices installed and a central authority, called the virtual credit center (VCC). As in many other incentive schemes for wireless networks and especially VANET (e.g., [15], [16] and [19]), the VCC is used. We assume that the VCC issues a certificate to each node and each node has an account (of virtual currency) in the VCC. Nodes do not need to connect to the VCC all the time. Instead, nodes save and store the information that they need to communicate with the VCC temporarily and when they are close to some infrastructures, they connect to the VCC and communicate with it (including receiving credits). For example, they can connect to the VCC in the gas station.

Initially, each node in the VANET system has an equal amount of virtual currency in its account stored by the VCC. If a node has helped in the forwarding of a message, whenever the node have chance to connect to the VCC, it submits the evidences (i.e., records of meetings and message receipts, which will be described in details later) to the VCC and receives the credits from the VCC. The VCC gives credits to a node in the form of virtual currency, i.e., it increases the amount of virtual currency that the node keeps in its account kept by the VCC. Correspondingly, the source node will be charged (the VCC decreases the amount of virtual currency in the source node's account). We note that in some cases, the source of a message may send it as a reply for a request for the benefit of the destination. We consider this problem as the incentive issues in the application layer, e.g., providing data service for others. There are some works on the incentive issues in the application layer (e.g., stimulating cooperation file sharing in peer-to-peer networks). We think that the incentive for the source to send packets and the incentive for the intermediate nodes to forward packets are two separate issues. The source is motivated by the incentive scheme in the application layer to send messages to the destination, while the intermediate nodes should also be incentivized in the network layer. Once the source is motivated by the application layer mechanism, it makes sense to let the source pay the forwarders since only when the data messages are delivered the source can receive rewards from the destination by the incentive scheme in the application layer. In this paper, we only focus on the incentive issues in the network layer. When a node needs more virtual money, it can buy some using real money. All transactions are cleared within the VCC. The details about how the VCC will process the evidences will be presented in Section IV-D.

B. Allocation of Payoff

Our goal is to design a payoff allocation method ($X \in \mathbf{R}^{\mathbf{N}}$) in the forwarding coalitional game such that for the transmissions of each message in VANETs, the grand coalition is guaranteed. To achieve the grand coalition, the challenge is to make sure the non-emptiness of the core in the game, and to assign a payoff allocation to each player in the coalition which satisfies the core requirement. Naturally, the source node and intermediate nodes should be treated differently in the payoff allocation, due to their different roles in the game. Therefore, we consider them separately.

1) Payoff Allocation to Intermediate Nodes: For each intermediate node, its share of payoff should reflect its contribution in the game. Hence the payoff allocation function for intermediate nodes, is designed as follows, based on two types of behaviors in the coalition, receiving and forwarding.

$$x_i = \alpha \cdot m_r(i) + \beta \cdot m_f(i) + u \cdot n_{rec}(i), \forall i \neq src. \quad (2)$$

In Eq. (2) $m_r(i)$ is the number of times that intermediate node i receives one copy of the message from some other node. $m_f(i)$ is the number of times that i successfully forwards one copy of the message to another node following the routing protocol $\Re$. α and β are the rewards for the receiving and forwarding behaviors respectively. $u \cdot n_{rec}(i)$ is the amount of reward to node i for reporting the meeting records. Note that $dest.$ can be viewed as an intermediate node, which only receives copies without further forwarding.

2) Payoff Allocation to The Source Node: The payoff allocation to the source node contains two parts: the gains by successfully delivering the message copies to $dest.$, subtracted by rewards used to pay the intermediate nodes. The payoff allocation function for $src.$ is defined in Eq. (3).

$$x_{src} = \delta \cdot d(\mathbf{N}) - (\alpha \sum_{i \in N - \{src\}} m_r(i) + \beta \sum_{i \in N - \{src\}} m_f(i)). \quad (3)$$

C. Sufficient Conditions to Achieve Core

With the payoff allocation functions described above, will the forwarding coalitional game automatically achieve a stable grand coalition? Actually it depends on the parameters δ, α and β. If the values of δ, α and β are chosen inappropriately, the core of the game may become empty. So in the sequel, we study how to choose the parameters and ensure that the payoff allocation of our incentive scheme is in the core, i.e., the payoff allocation satisfies individual rationality, coalitional rationality and efficiency respectively. At the end of this section, we summarize the results and give the sufficient conditions on δ, α and β for achieving the core.

1) Individual Rationality: First we examine the individual rationality of the players, i.e. no player receives less than what it could get on its own. For the source node, if it does not send the message to any intermediate node, then $v(\{src.\}) = 0$. Therefore, it is necessary to make sure that $x_{src.} \geq 0$ in grand coalition $\mathbf{N}$ whenever $d(\mathbf{N}) > 0$ to guarantee the individual rationality for the source node. [2].

Before introducing the parameter conditions for $src.$'s individual rationality, we define two terms m_r and m_f. Denote m_r, i.e. $m_r = \sum_{i \in \mathbf{N} - \{src.\}} m_r(i)$, the total number of receiving behaviors of intermediate nodes in grand coalition. Similarly, we let $m_f = \sum_{i \in \mathbf{N} - \{src.\}} m_f(i)$.

The following lemma specifies the condition to achieve individual rationality.

Lemma 3: If the equation Eq. (4) holds for the payoff allocation defined in (2) and (3), then the individual rationality is guaranteed.

$$max(\alpha, \beta) \leq \frac{\delta \cdot d(\mathbf{N})}{m_r + m_f}, \quad \text{whenever } d(\mathbf{N}) > 0 \tag{4}$$

Proof: For each intermediate node i, if it does not join the coalition, which means it does not record or forward any copy of the message, then $m_r(i) = 0$ and $m_f(i) = 0$. Hence $v(\{i\}) = 0$. Since in the definition of x_i (Eq. (2)) all components are non-negative, we have that $x_i \geq v(\{i\})$.

For the source node, it is easy to see that, if Eq. (4) holds, then

$$\begin{aligned} x_{src.} &= \delta \cdot d(\mathbf{N}) - (\alpha \cdot \sum_{i \in \mathbf{N} - \{src.\}} m_r(i) \\ &\quad + \beta \cdot \sum_{i \in \mathbf{N} - \{src.\}} m_f(i)) \\ &\geq \delta \cdot d(\mathbf{N}) - max(\alpha, \beta)(\sum_{i \in \mathbf{N} - \{src.\}} m_r(i) \\ &\quad + \sum_{i \in \mathbf{N} - \{src.\}} m_f(i)) \\ &= \delta \cdot d(\mathbf{N}) - max(\alpha, \beta) \cdot (m_r + m_f) \\ &\geq 0 \end{aligned}$$

Since $v(\{src\}) = 0$, the individual rationality for $src.$ is also guaranteed if $max(\alpha, \beta) \leq \frac{\delta \cdot d(\mathbf{N})}{m_r + m_f}$, whenever $d(\mathbf{N}) > 0$. ■

Given the result of Lemma 3, in designing our incentive scheme, we make $max(\alpha, \beta) = \frac{\delta \cdot d(\mathbf{N})}{m_r + m_f} - \varsigma$, where ς is a constant small number. Since we also need to guarantee that $\alpha > 0$ and $\beta > 0$, we choose ς such that $\varsigma < 1/(m_r + m_f)$.

2) Coalitional Rationality: Even with the individual rationality of each node, it still cannot guarantee that no coalition of nodes can benefit from deviating the grand coalition. To see this, we revisit the example in Figure 1 part (a). In this game, $m_r = 8$, $m_f = 7$. Let $\alpha = 0.55$, $\beta = 0.6$ to satisfy condition (4). Then in grand coalition the total payoff allocations that nodes in S_1 can get is $\sum_{i \in S_1} x_i = 13.25$, while the worth of the coalition S_1 is $v(S_1) = 15.5$. Intuitively, coalition S_1 can collectively get better payoff allocations by excluding nodes $2, 6, 7$ from their coalition and saving the payments to them, which worth 2.25 in total. Consequently, nodes in S_1 have the incentive to deviate from the grand coalition, which leads some nodes in $\mathbf{N}$ not to follow the routing protocol.

To overcome the difficulty in ensuring coalitional rationality, we modify the δ in Eq. (1), from a constant parameter to a function of the coalition S. $\delta(S)$ is the reward for successfully delivering one message copy in coalition S. In particular, define $\delta(S)$ as the ratio of the cooperative behaviors (receiving or forwarding) in S to the total number in $\mathbf{N}$.

$$\delta(S) = \frac{\sum_{i \in S - \{src.\}} (m_r(i) + m_f(i))}{m_r + m_f}.$$

In the grand coalition $\mathbf{N}$, all nodes are cooperative, so $\delta(\mathbf{N}) = 1$. Therefore the condition (4) can be rewritten as

$$max(\alpha, \beta) \leq \frac{d(\mathbf{N})}{m_r + m_f} \tag{5}$$

Now we are going to prove that given the condition (5), no node can benefit by deviating from the grand coalition and forming a coalition consisting of a subset of nodes.

Lemma 4: In the forwarding coalitional game $(\mathbf{N}, v)$, where $v(S) = \frac{\sum_{i \in S - \{src.\}} (m_r(i) + m_f(i))}{m_r + m_f} \cdot d(S) + u \cdot n_{rec}(S)$, the payoff allocations defined in (2) and (3) with condition that

$$max(\alpha, \beta) \leq \frac{d(\mathbf{N})}{m_r + m_f}$$

guarantee that no coalition has incentives to deviate from the grand coalition.

Proof: For coalition S that does not include $src.$ and $dest.$, it has only one member in S. Consequently the coalitional rationality is immediately guaranteed because it is equivalent to the individual rationality in this case.

Now consider an arbitrary coalition S. We compare the total value of the coalition S, $v(S)$ and the value sum of those nodes in S if they are in the grand coalition, $\sum_{i \in S} x_i$. If $\sum_{i \in S} x_i \geq v(S)$, it means that no subset of nodes can form a coalition obtaining higher total value than they are in the grand coalition.

$\forall S \subseteq N$, s.t. S contains $src.$ and $dest.$, we have

$$\begin{aligned} &\sum_{i \in S} x_i - v(S) \\ = \ & \frac{\sum_{i \in \mathbf{N}} (m_r(i) + m_f(i))}{m_r + m_f} d(\mathbf{N}) + n_{rec}(S) \\ & - \sum_{i \notin S} (\alpha m_r(i) + \beta m_f(i)) \\ & - \frac{\sum_{i \in S} (m_r(i) + m_f(i))}{m_r + m_f} d(S) - n_{rec}(S) \\ \geq \ & d(\mathbf{N}) - max(\alpha, \beta) \sum_{i \notin S} (m_r(i) + m_f(i)) \\ & - (1 - \frac{\sum_{i \notin S} (m_r(i) + m_f(i))}{m_r + m_f}) d(S) \\ \geq \ & \sum_{i \notin S} (m_r(i) + m_f(i)) (\frac{d(\mathbf{N})}{m_r + m_f} - max(\alpha, \beta)). \end{aligned}$$

[2]If $d(\mathbf{N}) = 0$, it means that although all involved nodes follow the routing protocol, $dest.$ still does not receive any copy of the message. In this case, $src.$ will get negative payoff allocation according to (3). But we argue that it is reasonable for $src.$, if it wants to transmit the message. Moreover, it is necessary to have this negative payoff allocation in order to prevent the cheating of $src.$ and $dest.$ in a collusion (see Section IV-E)

The last step of the above derivation is due to the fact that $d(\mathbf{N}) - d(S) \geq \frac{\sum_{i \notin S}(m_r(i)+m_f(i))}{m_r+m_f}(d(\mathbf{N}) - d(S))$.

Since $\sum_{i \notin S}(m_r(i) + m_f(i)) \geq 0$ and we have condition (5), we can obtain that $\sum_{i \in S} x_i - v(S) \geq 0$. Therefore, the coalitional rationality is guaranteed. ■

3) Efficiency: Finally it is easy to verify the efficiency of the payoff allocation. Actually

$$\begin{aligned} \sum_{i \in \mathbf{N}} x_i &= x_{src.} + \sum_{i \in \mathbf{N} - \{src.\}} x_i \\ &= \delta(\mathbf{N}) d(\mathbf{N}) + u \cdot n_{rec}(\mathbf{N}) = v(\mathbf{N}). \end{aligned}$$

We now summarize our analysis results in the following theorem.

Theorem 5: In the forwarding coalitional game $(\mathbf{N}, v)$, where

$$v(S) = \frac{\sum_{i \in S - \{src.\}}(m_r(i) + m_f(i))}{m_r + m_f} \cdot d(S) + u \cdot n_{rec}(S),$$

the payoff allocation X s.t., $\forall i \in N$

$$x_i = \begin{cases} \alpha \cdot m_r(i) + \beta \cdot m_f(i) + u \cdot n_{rec}(i) & \text{if } i \neq src. \\ d(\mathbf{N}) - (\alpha m_r + \beta m_f) & \text{otherwise,} \end{cases} \quad (6)$$

with the condition that

$$max(\alpha, \beta) = \frac{d(\mathbf{N})}{m_r + m_f} - \varsigma, \quad \text{if } d(\mathbf{N}) > 0 \quad (7)$$

is sufficient to be guaranteed in the core.

Proof: Due to Lemma 3, Lemma 4 and the efficiency analysis in Section IV-C3. ■

Theorem 5 guarantees that by using the payoff allocation functions, no coalition of the selfish nodes have the interest to break with the grand coalition. The system will converge to a strongly stable state that nodes are willing to follow the routing protocol and cooperate in forwarding messages.

D. Complete Design of Incentive Scheme

Based on the payoff allocation functions designed above, in this subsection we specify our complete incentive scheme.

We assume that there is a public key infrastructure in the VANETs. Each node i has a public/private key pair Kp_i, Ks_i and a certificate that is digitally signed by a trusted Certificate Authority. Denote $(sign_{Kp}(), verify_{Ks}())$ the digital signature scheme used in VANETs.

The complete incentive scheme consists of the programs installed at each node in the VANETs and the algorithm running at the VCC. The programs at each node can be further divided into three groups of functions, for the source node, the intermediate node and the destination, respectively. The detailed architecture of this incentive scheme is shown in Fig. 2.

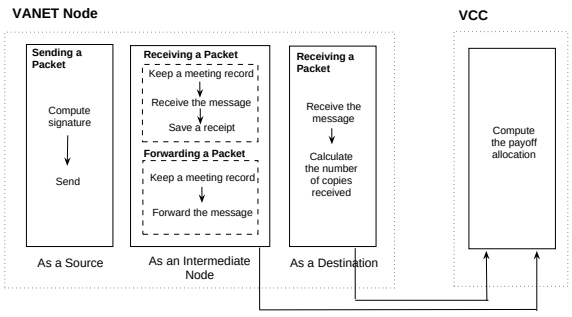


Fig. 2. Incentive scheme implementation architecture.

• **Source Node.** Suppose that $src.$ wants to send a message M to $dest.$. $src.$ computes a digital signature $sign_{Ks_{src.}}(md(M))$ based on the message it is about to send. $src.$ will send the message (or copies) together with the message-specific digital signature $sign_{Ks_{src.}}(md(M))$ to the adjacent intermediate nodes, where $md()$ is a message digest function.

• **Intermediate Nodes.** When a node carrying M meets a subsequent node, the two nodes first verify each other's identity using the authentication certificates. Each node keeps a brief record of their meeting $(ts, id, Rinf)$, where ts denotes the time when they meet. id is the identity of the other node, and $Rinf$ is the routing information available (that may needs to be exchanged with the other node in many routing protocols such as [10], [18]). Different content of $Rinf$ is defined according to the routing protocols used in VANETs. For example, if $\Re$ makes routing decisions based on historic meeting information [33], [10], [6], $Rinf$ can be the expected probabilities of meeting other nodes in the system.

If the node carrying M decides to forward according to routing protocol $\Re$, it sends the message M together with $sign_{Ks_{src}}(md(M))$ to the subsequent node. After receiving M, the subsequent node saves $sign_{Ks_{src}}(md(M))$ as a receipt. Nodes submits their meeting reports and message receipt to VCC whenever they can connect to it.

• **Destination Node.** If $dest.$ receives M or its copies, it waits for a certain amount of time and calculates the total number of copies it receives $d(\mathbf{N})$. When $dest.$ can connect to VCC, it submits its receipt, one copy of M together with $d(\mathbf{N})$ to the system.

• **Computing payoff allocations.** The VCC computes the payoff allocations once in a certain time interval, long enough to collect receipts and meeting reports. Whenever nodes can connect to VCC, they can receive their payoff allocations in form of credits. Before VCC starts to compute the payoff allocations, it first matches all meeting records into pairs by the same timestamp and corresponding node ids, and produce pairs of meeting record vectors in from of $(ts, id_1, id_2, Rinf_1, Rinf_2)$, $(ts, id_2, id_1, Rinf_2, Rinf_1)$. VCC discards the single meeting records which fail to match with any other ones. VCC counts the number of meeting records submitted by each node, and obtains each $n_{rec}(i)$ in the payoff allocation functions (6). Figure 3 specifies the protocol to compute the payoff allocations to the nodes who were involved in the transmission of message M. In order to compute the number of receiving and forwarding behaviors for each node, the protocol adopts a breath-first-search starting from $src.$ to trace all cooperative behaviors, using the meeting records information and receipts.

From Fig. 3, we can see that the algorithm to allocate payoff is essentially a breadth-first search of the message forwarding

tree. Therefore, the time complexity of the algorithm is $O(n)$, where n is the number of receipts that nodes in the system have submitted. Usually the number of n is depending on several factors, e.g., the total number of nodes in the network, the number of messages being transmitted, the basic routing protocol in the system, etc. [3]

→ Meeting record vectors
→ Receipts.
→ Routing protocol $\Re$ in the VANET.
→ A FIFO queue, Q, composed of IDs of nodes.

IF not received $d(\mathbf{N})$ from $dest.$
  $d(\mathbf{N}) \leftarrow 0$.
For each node i, $m_r(i) \leftarrow 0$; $m_f(i) \leftarrow 0$.
Add $src.$ to Q.
WHILE (Q is not Empty){
  Take an id $id_{current}$ out of Q.
  IF not found any $(ts, id_1, id_2, Rinf_1, Rinf_2)$
    s.t. $id_1 = id_{current}$
    BREAK.
  ELSE FOR each $(ts, id_{current}, id_2, Rinf_1, Rinf_2)$
    IF found receipt from id_2
      Based on $Rinf_1, Rinf_2$ check whether the
        forwarding between $id_{current}$ and id_2 follows $\Re$.
      IF not legal, **BREAK**.
      ELSE
        $m_f(id_{current})$++; $m_r(id_2)$++; Add id_2 to Q.
}
$m_r \leftarrow \sum_i^N m_r(i)$; $m_f \leftarrow \sum_i^N m_f(i)$.
FOR each $i \neq src.$
  $x_i \leftarrow \alpha m_r(i) + \beta m_f(i) + u \cdot n_{rec}(i)$.
$x_{src.} \leftarrow d(\mathbf{N}) - \alpha m_r - \beta m_f$.

Fig. 3. Protocol to compute the payoff allocations in one game

E. Preventing Cheating Behaviors

In Section IV-C the analysis shows that the payoff allocation functions in our incentive scheme stimulate the nodes to cooperate. However nodes may still cheat by submitting false information that is used in computing the payoff allocations. In this subsection, we analyze the possible false information that nodes may submit and discuss solutions to prevent these cheating behaviors.

• **False receipts.** Since the payoff allocation of each node in the system essentially depends on the number of receipts that they submit, nodes may save and submit the receipts without forwarding the message. If the nodes behave like this, it will cause the number of copies delivered to $dest.$ less than what it should be. In this case, according to the payoff allocation condition (7), the amount of payoff allocation that each intermediate node gets decreases as $d(\mathbf{N})$ drops. So by carefully choosing parameters α and β, it can be guaranteed that nodes get punished by losing their payoff shares.

• **False d(N).** Now we consider the case that $dest.$ reports false $d(\mathbf{N})$ in collusion with $src.$. Since if $d(\mathbf{N})$ is higher, $src.$ can get more payoff shares, $dest.$ may declare to receive more than $d(\mathbf{N})$ copies. Actually, our payoff allocation computing protocol can prevent this cheating behavior. Because the protocol traces all effective routes and verifies all forwarders' receipts, any false $d(\mathbf{N})$ will be detected.

• **False meeting records.** According to our analysis in Section IV-C hiding meetings records and not following the routing protocol will not result in higher payoff shares for the nodes. Therefore, the remaining problem is to prevent them from forging false meeting records which have not really happened.

There are two types of forged meeting records: 1) meeting records with false time and meeting nodes ids, i.e. totally forged meeting records; 2) meeting records only with false routing information. One node cannot generate a totally forged meeting record by itself, because our protocol discards all non-paired records as mentioned above. If two nodes collude in generating false routing information, they can transfer more messages that are not allowed by $\Re$, and hence obtain more payoff allocations than they should. To prevent this kind of cheating behavior, different solutions for different routing protocols are needed. If $\Re$ is based on historic transfer information, (e.g., some $\Re$ bounds the number of replicates of one message), our protocol can detect the forged information since it can verify and record all legal forwardings in the breath-first search. In some other $\Re$s, nodes exchange control information, for instance the expected transfer probabilities. To enforce the nodes to honestly measure and report routing information, similar approaches to those in [31] can be adopted.

V. Extended Scheme

In this section, we extend our incentive scheme to address the challenge brought by the limited storage space of nodes. Indeed, storage space is more available for VANETs nodes than traditional multi-hop wireless network nodes. However, it could still be limited since there may be a lot of applications running inside the vehicles which could also consume storage space. It is not likely that the vehicle owner would buy a lot of extra storage space for carrying data messages for other nodes, especially when it can decide the space capacity. Therefore, we believe that under some circumstances, storage space could still be limited for message forwarding in VANETs. Most existing routing protocols (such as [18], [34]) have taken limited storage into consideration; they disseminate some control information to make the decision on how to better utilize the storage space. Consequently, a theoretical solution would be extending our incentive scheme to guarantee the cooperation in truthfully reporting and transferring control information. Nevertheless, such a theoretical solution suffers from a very large overhead. So, in this section, we provide an alternative light-weight incentive approach to solve this problem. Specifically, we extend the payoff allocation functions in the incentive scheme, so that the system can intentionally choose a performance metric to optimize and distribute the payoff to each node according to how its forwarding behavior satisfies the routing goal. As the nodes are selfish and aim to maximize the total payoff shares of their own, we show that it is their dominant strategies [32] to always drop the messages that the system prefers to drop.

It is assumed that in a VANET, nodes only have limited space to store at most P messages. Hence, although forwarding more messages will bring them higher payoff shares, nodes

[3]Note that the algorithm of the VCC is running on backend machines, so the computing ability of the VCC is not a major concern here.

can only carry some of those that they receive. We classify the time to discard a message into two categories: before meeting the subsequent node and after forwarding to the subsequent node. Clearly, in the first case, the forwarding behavior does not occur while in the second case it occurs. Recall that transmission of each message from source to destination is modeled as a forwarding coalitional game. We assume there are Q messages, with different sources or destinations, transferred in the VANET. Therefore there are Q games that a node could possibly participate. Denote G the game set, and $|G| = Q$. Each game g in G can be labeled by the source-destination pair.

We now extend the payoff allocation functions in our incentive scheme. The payoff allocation of node i in game g is defined as

$$x_i(g) = \alpha_i(g) \cdot m_r(i,g) + \beta_i(g) \cdot m_f(i,g) + u \cdot n_{rec}(i,g), \quad (8)$$

where $\alpha_i(g)$ (resp. $\beta_i(g)$) is the amount of reward that i can obtain for receiving (resp. forwarding) a message copy in game g. In words, we change the constant unit reward to a reward function on the player and the game. When the game g ends, VCC computes $\alpha_i(g)$ and $\beta_i(g)$ first, before allocating the payoffs.

The design of $\alpha_i(g)$ and $\beta_i(g)$ depends on which performance metric that the system wants to optimize and the corresponding routing protocol. Here we present an example of $\alpha_i(g)$ and $\beta_i(g)$ for systems aiming to maximize the delivery ratio. Define

$$\alpha_i(g) = \beta_i(g) = (d_g(\mathbf{N}) - d_g(\mathbf{N} - \{i\})) \cdot m_f(i,g) \cdot \gamma,$$

where $d_g(\mathbf{N})$ denotes the number of message copies delivered to the destination in game g, and $d_g(\mathbf{N} - \{i\})$ is the number of delivered copies if the node i is excluded from the game. γ is a constant parameter used to scale the total payoff. Intuitively, if $d_g(\mathbf{N}) - d_g(\mathbf{N} - \{i\}) = 0$, it means that the node contributes nothing to the delivery of message. $d_g(\mathbf{N} - \{i\})$ can be computed in the VCC using the meeting records submitted by the nodes. Greater $\alpha_i(g)$ and $\beta_i(g)$ imply that the receiving and forwarding of node i result in higher delivery ratio.

With the above extension, the total payoff shares that a player can obtain in the Q games is $X_i = \sum_{g \in G} x_i(g)$. In the following theorem, the dominant strategy of each node is to contribute more in the games which can bring higher payoff shares to it.

Theorem 6: Assume that for each game g, the payoff share for node i is defined as Eq. (8), and $\alpha_i(g) \propto \beta_i(g) \propto m_f(i,g)$. Then it is a dominant strategy for each node to accept the messages with highest $\alpha_i(g)$ during a transfer opportunity and to remove the messages with lowest $\beta_i(g)$ to make room for the incoming messages.

Proof: Denote s^* the strategy such that nodes accept the messages with highest $\alpha_i(g)$ during a transfer opportunity and remove the messages with lowest $\beta_i(g)$ to make room for the incoming messages. There are two cases of strategy s' s.t. $s^* \neq s'$.

Case 1. Let s' denote the strategy that in some transfer opportunity, the node decides to accept a message in g' instead of g s.t. $\alpha_i(g') < \alpha_i(g)$. Other actions are the same as in s. Then for player i the total payoff allocation difference of taking strategy s' and s is

$$\begin{aligned} & X_i(s'_i) - X_i(s^*) \\ = \; & \alpha_i(g') - \alpha_i(g) + \beta_i(g') \cdot m_f(i,g') - \beta_i(g) \cdot m_f(i,g) \\ \leq \; & 0. \end{aligned}$$

Case 2. Let s'' denote the strategy that in some transmission, in order to make room for the incoming messages, the node remove a message g' instead of g, s.t. $\beta_i(g') > \beta_i(g)$. We can obtain that

$$X_i(s''_i) - X_i(s^*) = \beta_i(g) \cdot m_f(i,g) - \beta_i(g') \cdot m_f(i,g') \leq 0.$$

Therefore, strategy s^* is a dominant strategy for each node. ■

We note that $\alpha_i(g)$ and $\beta_i(g)$ are computed by the VCC after the game g ends, and the knowledge of $\alpha_i(g)$ and $\beta_i(g)$ is not forwarded in the VANETs to reach node i. Then how can each node know $\alpha_i(g)$ and $\beta_i(g)$ in order to maximize its own total payoff? Actually each node can approximate the parameters using the local information and what it receives from the VCC. There are a lot of algorithms that nodes can apply to estimate $\alpha_i(g)$ and $\beta_i(g)$ for each game. The key idea is that if in history a node got high unit payoff from forwarding for a source-destination pair, it is likely that this trend will last for some time as long as its mobility pattern does not change dramatically. Here by mobility pattern we mean the path followed by a vehicle during an extensive time frame. Based on its historic behaviors and the corresponding payoff shares, nodes can estimate $\alpha_i(g)$ and $\beta_i(g)$ in the current game. After the nodes learn for long enough time, the system will converge to the equilibrium in which nodes take their dominant strategies and meanwhile the system objective can be met. For example, one VANET node passes by a department store every morning and afternoon on the way between home and office, and this department store regularly disseminates the announcement of sale information. Hence this node can learn from its previous experience that helping forwarding the messages for the department store gains more payoffs than for other unknown sources. Therefore it can decide which message to discard if space is limited, to the best of its own interest. We will verify this by the experiments in Section VI-D.

VI. Evaluation

In this section, we extensively evaluate our incentive scheme using GloMoSim [35]. Our objectives are two folds: a) to verify that our scheme effectively stimulates cooperation in VANETs, b) to evaluate the impact of our scheme in improving the system performance in terms of delivery ratio and delay time, when selfish behaviors appear in VANETs. The experiments are conducted on the traces from a real vehicular network, DieselNet [6]. We test our incentive scheme based on two different routing protocols, MV [10] and binary Spray-and-Wait [11]. In Section VI-D, we also evaluate the performance of our incentive scheme with limited storage space of nodes.

A. Settings

• **Traces from DieselNet.** We evaluate our incentive scheme on testbed traces from DieselNet [6]. It is a vehicular network testbed consisting of 40 buses, of which only a subset is on the road each day. Each bus in DieselNet carries a computer of 40G storage space and a GPS device. They are set to transmit random data to other nodes whenever they are within the range. The traces from Feb 6, 2007 until May 14, 2007 [18] (58 files) are used. These traces are from the buses running routes serviced by UmassTransit. The mobility of these buses are determined by UmassTransit and the bus routes can be found at $http://www.umass.edu/campus\_services/transit/$. The average number of meetings between buses per day is 147.5. Each tracefile consists of the connection events occurring during a day. For each meeting event, the following information is recorded as a tuple: the MAC address of the bus sending data, the MAC address of the bus receiving data, the time of meeting, transmission size and meeting location. The traces are generated using a default rate of 4 messages per hour of each bus for every other bus on the road and the size of each message is 1KB. We import the traces of 11 buses each day into GloMoSim, and vary the message generating rate in our experiments. The experiment results are averaged over 58 traces.

• **Routing protocols.** In each of the VANET network, we test our incentive scheme with two different routing protocols, MV and binary Spray-and-Wait. The objective of using two routing protocols in our evaluation is not to compare them, but to show that our incentive scheme can guarantee packet forwarding cooperation for the systems with different routing protocols. Although MV and Spray-and-Wait are initially designed for delay-tolerant routing, they are also very useful in the multi-hop delay-tolerant scenarios for vehicular networks, such as delivering commercial advertisements regarding sale information at a store, with low vehicle density. We choose these two protocols because each of them is representative in the two categories of routing protocols (See Section II). The key idea of MV is to estimate the delivery probability of each node to the message destination using historic contact information, while Spray-and-Wait is based on message replication but restricts the number of copies for each message to L. In the experiments on MV, the time unit in calculating the delivery probabilities is set to 1 minute and node do not keep copies after forwarding them. In binary Spray-and-Wait set $L = 12$.

• **Metrics.** To show that our incentive scheme indeed provides effective stimulation for forwarding cooperation, we measure the *accumulative credit* of the forwarding nodes when they have different forwarding behaviors. Note that nodes have to spend credits to send their own messages, so they have the incentive to earn more credits for future use. Our incentive scheme computes payoff allocations every 30 minutes. Set $u = 0.01$, $\beta = \frac{d(\mathbf{N})}{m_r+m_f} - 0.02$ and $\alpha = \beta - 0.05$. We set u, β and α as above because we need to guarantee that $\alpha > 0$, $\beta > 0$ and $\max(\alpha, beta) \leq \frac{d(\mathbf{N})}{m_r+m_f}$. In addition, we let $\alpha < \beta$ due to the reason that the behavior of forwarding a message requires not only sending it but also storing the message until meeting the subsequent node. Hence it makes sense to reward a little more to the behavior of forwarding. We set the value of u relatively small because making meeting records requires less energy consumption than receiving and forwarding data messages. To evaluate the impact of our incentive scheme on the system performance, we measure both *delivery ratio* and *delay time*.

Nodes use IEEE 802.11 (at 11Mbps) as the MAC layer protocol. The radios' transmission range is set to 250 meters. The radio propagation model is two-way.

B. Accumulative Credit

The first set of experiments is to verify that with our incentive scheme, nodes always lose credits if they do not faithfully follow the routing protocols. Specifically, we define the selfish behavior as only forwarding the messages destined to the nodes in its own coalition. In other words, selfish nodes do not follow routing protocol if the incoming message is not destined within its coalition. We vary the size of the coalition which consists of selfish nodes, and all other nodes remain cooperative. We set up two different coalition scenarios for the selfish users. The first scenario is that there are two coalitions in total, with one of size 6 and the other of size 5. The second scenario is that the 11 active nodes form 3 coalitions, consisting of 4 nodes, 4 nodes, and 3 nodes respectively. We record the average accumulative credits of selfish nodes in coalitions of different sizes and compare them with the average accumulative credits of cooperative nodes.

Figure 4 and Figure 5 respectively show the results of MV and Spray-and-Wait in DieselNet. We can observe that at any time, nodes get the most credits if they cooperatively follow the routing protocol for all the messages. The smaller the coalition is, the less credits can the selfish nodes obtain. Note that because the buses only operate in the daytime, the credits of the nodes remain the same when there are no messages transmissions taking place. From the figures it is clear that with either MV or Spray-and-Wait applied in the network, selfish nodes can never receive more credits than cooperatively forwarding all the messages. Therefore, our incentive scheme provides an effective stimulating mechanism for nodes to cooperate.

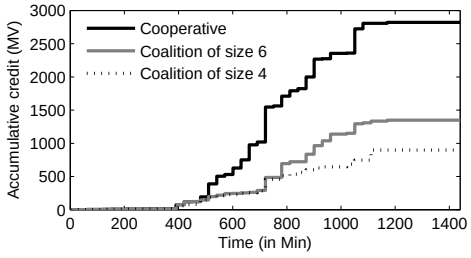


Fig. 4. (MV) Accumulative credit of node in coalition of different sizes v.s. cooperative nodes.

C. Impacts on System Performance

Our second set of experiments is to show that when the network has selfish nodes, our incentive scheme can improve

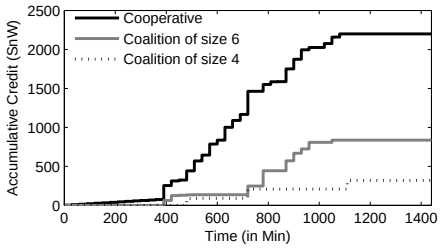


Fig. 5. (Spray-and-Wait) Accumulative credit of node in coalition of different sizes v.s. cooperative nodes.

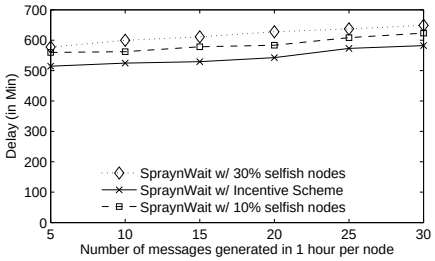


Fig. 7. Delivery ratios achieved with and without our incentive scheme when Spray-and-Wait is used.

the system performance. In particular, we demonstrate how the incentive scheme can impact the delivery ratio and delay time when 30% and 10% of the nodes in the VANET are selfish. The selfish nodes are randomly picked and the selfish behavior is defined the same as above.

We vary the message generating rate and measure the delivery ratio and the average max-delay time per message. Figure 6 and Figure 8 shows the results of the experiments on MV, and Figure 7 and Figure 9 demonstrates the results on Spray-and-Wait. As shown in Figure 6, our scheme increases the delivery ratio of MV routing protocol by up to 23.9%, when there are 30% nodes form a coalition in the network. We also find that when there are 10% nodes in the system, the delivery ratio is higher than the case of 30% selfish nodes. Similar conclusion can be drawn from Figure 7 that our incentive scheme can increase the delivery ratio of Spary-and-Wait by up to 9.44% when there are 30% selfish nodes. Furthermore, it can be seen from Figure 8 and Figure 9 that our incentive scheme can always shorten the average max-delay time of messages (up to 9.5% for MV, and up to 14.5% for Spray-and-Wait). Again more selfish nodes in the system result in longer delay time.

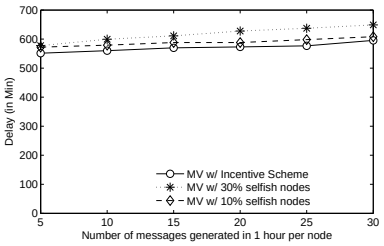


Fig. 6. Delivery ratios achieved with and without our incentive scheme when MV is used.

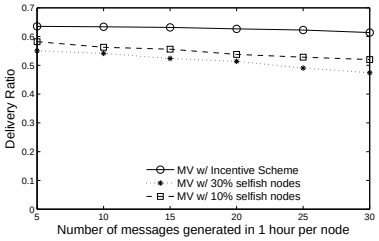


Fig. 8. Average delay of messages in the system with and without our incentive scheme when MV is used.

D. Experiments on Extended Scheme

In this subsection, we evaluate our extended scheme when the nodes only have limited storage space. We assume that all nodes are cooperative in that they always receive and forward the packets for others, and compare the results of two sets of experiments. In one set, we let the nodes randomly drop messages when the storage space is full, while in the other set, we let nodes learn from the credits received in history, and keep the message destined to the most profitable destinations to them. The cooperative nodes learn from the credits received in history, and keep the message destined to the most profitable destinations to them. The noncooperative nodes just randomly choose some of the messages in the storage space to drop.

Figure 10 represents the system delivery ratios when the system converges to the stable state. We vary the storage capacity from 50 messages to 250 messages and compare the results from the two dropping behaviors. It is can be observed that cooperative behavior always results in higher delivery ratio than random dropping. The difference is more significant when the storage space is smaller. Hence, we can conclude that the cooperative dropping behavior can increase the system delivery ratio compared with randomly dropping.

Figure 11 shows the accumulative credits of the cooperative and random behaviors. It is clear that at any time, the cooperative behavior brings the nodes more credits than randomly dropping. Therefore, the extended scheme indeed encourages the nodes to cooperatively drop messages.

E. Overhead

In this subsection, we examine the overhead introduced by our scheme. For mobile nodes, we focus on the storage space occupied by our scheme and the overhead for making meeting records. For the VCC, we examine the time to calculate the credit for each node. We assume that mobile nodes can connect with the VCC once a day. We use crypto++ 5.5.2 [36] for the cryptographic scheme implementation. The tests are performed on a laptop Intel Core 2.67 GHz processor under Windows Vista in 32-bit mode. **Communication Overhead** We use Elliptic Curve Cryptography (ECC) for the PKI implementation. We set the key length of ECDSA to 192 bits, and the digital signature of each message digest is 48 bytes. Assume the length of the message is x bytes, and the

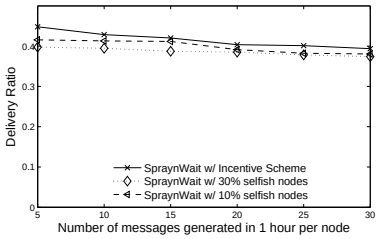


Fig. 9. Average delay of messages in the system with and without our incentive scheme when Spray-and-Wait is used.

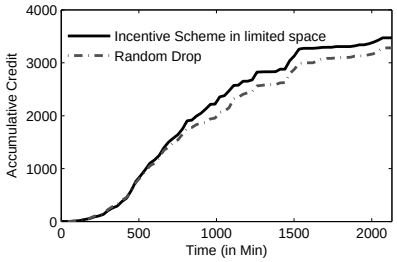


Fig. 11. Accumulative credit of the nodes. Following our extended scheme vs. random strategy to drop messages.

Fig. 10. Delivery Ratio in experiments on extended scheme as function of different space limits.

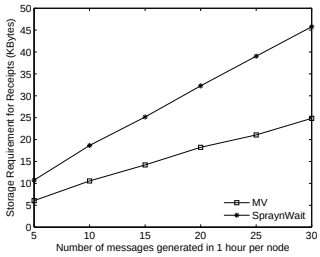


Fig. 12. Storage requirement for saving receipts on each node.

total length of the data message is $(48 + x)$ bytes. In our experiments, $x = 1000$, so the communication overhead for data transmission is about 4.6%.

For the authentication process when two nodes meet, we also use 48 bytes ECDSA certificate. On average, it requires 6.38 mseconds for the verification per node.

Storage Requirement In our scheme, the storage requirement comes from two parts: meeting records and message receipts that nodes need to keep before connecting to the VCC.

The average storage usage for meeting records on each node is 118.4 bytes.

We evaluate the storage requirement for message receipts with different message rates per node, and show the results in Figure 12.

As we can see that the space requirements for storing message receipts are very small per node. For MV protocol the storage overhead is within the range of (5,25) KBytes when the number of per-hour messages changes from 5 to 30. SpraynWait protocol requires more storage, ranging from 10 to about 45 KBytes.

Computation Overhead on VCC We measure the time to compute the allocation of credits for all nodes in the VCC as shown in Figure 13. When there are more messages generated in the system, the VCC uses more time to verify each message forwarding behavior and correspondingly allocate the credits to each cooperative nodes. Overall, it is very fast for VCC to conduct such computation within about one minute.

VII. Conclusion

In this paper, simple and effective incentive scheme in VANETs is proposed to stimulate the forwarding cooperation of nodes. We are the first to present an incentive scheme for VANETs with theoretical guarantee. We formally prove, in a coalitional game model, that with our scheme every relevant node cooperates in forwarding messages as required by the routing protocol. An extension is made to scenarios with constrained storage space, and a light-weight approach to stimulate cooperation is proposed. We integrate our incentive scheme with MV and Spray-and-Wait respectively and evaluate the system performance on testbed traces. The experimental results show that our incentive scheme provides effective stimulation for nodes to cooperate and prevents the degradation of system performance in VANETs with selfish nodes. Although our work provides theoretical guarantee on the cooperation, we only test it using testbed traces. In the future, more testbed experiments in the real world are needed to further verify our schemes and improve the design based on real implementation problems.

In designing our schemes, we assume that there are no communication failures for the control messages at physical level of each link. However, in reality, the communication capacity is affected by conditions related to the environment, e.g., shadow fading. [37], [38], [39] It means that in the inter-vehicle communications of our scheme (e.g., identity verification and making meeting records), errors may occur due to failures of physical lever and thus consequently the link drops. The authors of [40] proved that the error probability is log-concave for a wide class of multidimensional modulation formats. Based on this finding, they derived nice results on upper and lower bounds, and local bounds that are tight in a given region of interest for the error probability. In [41], a thorough discussion about the impact of bit error rates of links on the quality of different traffic types in VANETs is provided. All the works above show that the performance of our incentive scheme could be affected by the physical level communication failures. In particular, if the communication failure occurs when the nodes have made meeting records but

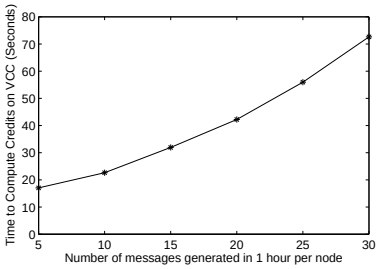


Fig. 13. Time to compute credits on VCC.

the data transmission has not finished, the VCC will allocate inaccurate amount of credits to the intermediate nodes, since the destination cannot receive the correct data in this case.

In our future work, we hope to reduce the impact of communication failures on our incentive schemes. We can work towards the following two directions: a) We will try to further reduce the length of communication overhead introduced by our schemes. In this way, the probability of link failures occurring in transmitting control information can be reduced; b) We can leverage existing physical layer techniques in wireless networks to estimate the link residual time based on the surrounding conditions. Consequently, more accurate calculations of credits can be conducted on the VCC.

REFERENCES

[1] D. Reichardt, M. Miglietta, L. Moretti, P. Morsink, and W. Schulz. CarTALK 2000 - Safe and Comfortable Driving Based upon Inter-Vehicle-Communication. IEEE Intelligent Vehicle Symposium, 2002.

[2] X. Yang, J. Liu, F. Zhao, and N. Vaidya. A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning. MobiQuitous, 2004.

[3] Q. Xu, T. Mark, J. Ko, and R. Sengupta. Vehicle-to-Vehicle Safety Messaging in DSRC. ACM Workshop VANET, 2004.

[4] J. Luo and J.-P. Hubaux. A Survey of Research in Inter-Vehicle Communications. Securing Current and Future Automotive IT Applications, pp 111-122, Springer-Verlag, 2005.

[5] J. Ott and D. Kutscher. A Disconnection-Tolerant Transport for Drive-thru Internet Environments. *In Proc. INFOCOM'05*, Mar. 2005.

[6] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine. MaxProp: Routing for Vehicle-Based Disruption- Tolerant Networks. *In Proc. INFOCOM'06*, April 2006.

[7] E. Jones, L. Li, and P. Ward. Practical Routing in Delay-Tolerant Networks. *In Proc. ACM Chants Workshop*, Aug. 2005.

[8] S. Jain, K. Fall, and R. Patra. Routing in a Delay Tolerant Network. *In Proc. SIGCOMM'04*, pages 145-158, 2004.

[9] A. Vahdat and D. Becker. Epidemic routing for partially connected ad hoc networks. Technical Report CS-200006, Duke University, April 2000.

[10] B. Burns, O. Brock, and B. N. Levine. MV Routing and Capacity Building in Disruption Tolerant Networks. *In Proc. INFOCOM'05*, March 2005.

[11] T. Spyropoulos, K. Psounis, and C. S. Raghavendra. Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks. *In Proc. WDTN'05*, Aug. 2005.

[12] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proc. MOBICOM00*, Boston, MA, Aug. 2000.

[13] P. Michiardi and R. Molva. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proc. CMS'02* Portoroz, Slovenia, Sep. 2002.

[14] M. T. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy. A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In *Proc. MobiQuitous'05*, San Diego, CA, Jul. 2005.

[15] S. Zhong, J. Chen, and Y. R. Yang. Sprite, a simple, cheat-proof, credit-based system for mobile ad-hoc networks. *In Proc. of INFOCOM'03*, San Francisco, CA, Apr. 2003.

[16] S. Zhong, L. Li, Y. Liu, and Y. R. Yang. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks-an integrated approach using game theoretical and cryptographic techniques. In Proceedings of ACM MobiCom Cologne, Germany, Sept. 2005.

[17] U. Shevade, H. H. Song, L. Qiu, Y. Zhang. Incentive-Aware Routing in DTNs. *In Proc. ICNP'08*, Oct. 2008.

[18] A. Balasubramanianm, B. N. Levine and A. Venkataramani, DTN Routing as a Resource Allocation Problem in *Proc. of SIGCOMM'07*, Aug. 2007.

[19] S. Lee, G. Pan, J. Park, M. Gerla, S. Lu. Secure incentives for commercial ad dissemination in vehicular networks. In *Proc. of MOBIHOC'07*, Sep. 2007.

[20] F. Li and J. Wu, FRAME: An Innovative Incentive Scheme in Vehicular Networks, in *Proc. of IEEE International Conference on Communications (ICC)* , 2009.

[21] T. Spyropoulos and K. Psounis and C. Raghavendra. Single-copy Routing in Intermittently Connected Mobile Networks. In *Proc. of SECON'04*, Oct. 2004.

[22] J.J. Jaramillo and R. Srikant. DARWIN: Distributed and Adaptive Reputation mechanism for WIreless ad-hoc Networks. In *Proc. MOBICOM07*, Montreal, Quebec, Canada. Sep. 2007.

[23] W. Wang, X.-Y. Li, Y. Wang, Z. Sun Designing Multicast Protocols for Non-Cooperative Networks, IEEE JSAC, January, 2008.

[24] WeiZhao Wang, Stephan Eidenbez, Yu Wang and Xiang-Yang Li. OURS- Optimal Unicast Routing Systems in Non-Cooperative Wireless Networks. In *Proc. of ACM MobiCom* 2006.

[25] X-Y Li, Y. Wu, P. Xu, G. Chen, and M. Li Hidden Information and Actions in Multi-Hop Wireless Ad Hoc Networks ACM MobiHoc 2008.

[26] M. E. Mahmoud and X. Shen. PIS: A Practical Incentive System for Multi-hop Wireless Networks, *IEEE Trans. on Vehicular Technology*, in press, 2010.

[27] T. Chen and S. Zhong, INPAC: An Enforceable Incentive Scheme for Wireless Networks using Network Coding, in *Proc. of INFOCOM'10*.

[28] B. Parno and A. Perrig. Challenges in Securing Vehicular Networks. HotNets-IV, 2005.

[29] M. Raya and J.-P. Hubaux. The security of Vehicular Ad Hoc Networks. ACM Workshop SASN, 2005.

[30] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security Issues in a Future Vehicular Network. EuroWireless, 2002.

[31] F. Wu, T. Chen, S. Zhong, L. Li and Y. R. Yang. Incentive-Compatible Opportunistic Routing for Wireless Networks. In *Proc. of MOBICOM'08*, San Francisco, CA, Sep. 2008.

[32] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*. The MIT Press, 1994.

[33] J. Davis, A. Fagg, and B. N. Levine. Wearable Computers and Packet Transport Mechanisms in Highly Partitioned Ad hoc Networks. In *Proc. IEEE ISWC*, pages 141-148, Oct. 2001.

[34] P. Hui, J. Crowcroft and E. Yoneki. BUBBLE Rap: Social-based Forwarding in Delay Tolerant Networks. In *Proc. of ACM MOBIHOC'08*, May, 2008.

[35] UCLA GloMoSim project, http://pcl.cs.ucla.edu/projects/glomosim/.

[36] W. Dai. Crypto++5.5.2. Available at http://www.eskimo.com/weidai/ cryptlib.html.

[37] A.J., Goldsmith and Soon-Ghee Chua, Variable-rate variable-power MQAM for fading channel, in *IEEE Trans. Commun.*, vol. 45, no. 10, pp. 1218-1230, Oct. 1997.

[38] A. Conti, M. Z. Win and M. Chiani, Slow AdaptivM-QAM With Diversity in Fast Fading and Shadowing,*IEEE Trans. Commun.*, vol. 55, no. 5, pp. 895-905, May 2007.

[39] A. Conti,W. M. Gifford,M. Win, M. Chiani, Optimized simple bounds for diversity systems, *IEEE Trans. Commun.*, vol. 57, no. 9, pp. 2674-2685, Sep. 2009.

[40] A. Conti, D. Panchenko, S. Sidenko and V. Tralli Log-concavity property of the error probability with application to local bounds for wireless communications, in *IEEE Transactions on Information Theory*, 55-6, 2766-2775, 2009.

[41] A. Conti, O. Andrisano, B, M. Masini and A. Bazzi, Chapter 4: Heterogeneous Wireless Communications for Vehicular Networks, in *Vehicular Networks: Techniques, Standards, and Applications*, ISBN:978-1-4200-8571-6.

Tingting Chen received her B.S. and M.S. degrees in computer science from the department of computer science and technology, Harbin Institute of Technology, China, in 2004 and 2006 respectively. She is currently a Ph.D. candidate at the department of computer science and engineering, the State University of New York at Buffalo, U. S. A. Her research interests include data privacy and economic incentives in wireless networks.

Fan Wu is an assistant professor in the Department of Computer Science and Engineering at Shanghai Jiao Tong University. He received the BS degree in computer science from Nanjing University in 2004 and the PhD degree in computer science and engineering from the University at Buffalo, the State University of New York, in 2009. His research interests include wireless networking, economic incentives for cooperation, and peer-to-peer computing. He is a member of the IEEE.

Sheng Zhong is an associate professor at the computer science and engineering department of the State University of New York at Buffalo. He received his BS (1996), ME (1999) from Nanjing University, and PhD (2004) from Yale University, all in computer science. His research interests include privacy and incentives in data mining and databases, economic incentives in wireless networks.