IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 15, 2020, accepted January 12, 2021, date of publication January 18, 2021, date of current version January 25, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3051976

Quantitative Study on Impact of Static/Dynamic Selfishness on Network Performance in VANETs

AXIDA SHAN[1,2], (Graduate Student Member, IEEE), XIUMEI FAN[1], (Member, IEEE), CELIMUGE WU[3], (Senior Member, IEEE), AND XINGHUI ZHANG[1,4]

[1]Department of Automation and Information Engineering, Xi'an University of Technology, Xi'an 710048, China
[2]School of Information Science and Technology, Baotou Teachers' College, Baotou 014030, China
[3]Graduate School of Informatics and Engineering, The University of Electro-Communications, Tokyo 182-8585, Japan
[4]College of Electronic and Information Engineering, Ankang University, Ankang 725000, China

Corresponding author: Xiumei Fan (xmfan@xaut.edu.cn)

This work was supported in part by ROIS NII Open Collaborative Research under Grant 2020-20S0502, in part by JSPS KAKENHI under Grant 18KK0279, Grant 19H04093, and Grant 20H00592; and in part by the National Natural Science Foundation of China under Grant 61272509.

ABSTRACT Vehicular ad hoc network is a kind of mobile ad hoc networks which provides wireless communication between vehicles. In most cases, multi-hop communication is needed, because of the limited range of wireless transmission. The multi-hop communication among nodes strictly relies on the forwarding functionality of intermediate nodes. Due to resource limitation, the intermediate nodes may exhibit selfishness and refuse to bear forwarding tasks for others. In this article, we defined two types of selfish nodes, namely static selfish nodes and dynamic selfish nodes. The impact of the two types of selfish nodes are quantitatively investigated from various aspects including mobilities, proportions, densities, and combinations. We conducted exhaustive simulations on an integrated simulation platform which consists of OMNeT++, SUMO, INET, and Veins. The experimental results indicate that the static selfish nodes have more harmful impacts on the performance of vehicular ad hoc networks in terms of average packet delivery ratios and end-to-end delays. Moreover, the results also imply that the impact of node selfishness should be evaluated by a comprehensive consideration of mobilities, proportions, densities, and combinations of selfish nodes.

INDEX TERMS Forwarding, impact, OMNeT++, selfish nodes, vehicular ad hoc network.

I. INTRODUCTION

Intelligent transportation systems (ITS) is the future direction of the transportation system which aims to provide better services for drivers and riders. Vehicular ad hoc network (VANET) [1], an expansion of mobile ad hoc networks (MANET), provides wireless communication between vehicles over wireless communication links without the assistance of any trusted authorities (TA) in ITS. VANET is a multi-hop wireless network that consists of a set of autonomous, self-organized, resource-limited, and mobile wireless vehicles (the terms, nodes and vehicles, are interchangeable in this work) to provide information sharing services for ITS including safety and non-safety (infotainment) applications [2]. Similar to MANETs, each node in a VANET functions as a normal host and is also responsible to perform routing operations [3]. The network topology of VANETs changes dynamically, because the connectivity among nodes is inevitably influenced by the nodes' mobility, departure, and arrivals. As a result, the communication efficiency highly depends on the cooperation of intermediate nodes in the routing path. Hence, efficient routing protocols in VANETs could provide effective communication among nodes based on fully utilization of the intermediate nodes [4]. However, these routing protocols share a common assumption that all nodes are naturally cooperative in VANETs. In practice, due to the restricted bandwidth and lack of computational resources, it is difficult to ensure every node in the network is altruistic to share out own precious resources to others. Hence, the assumption is not practical in a VANET environment [5]. The non-cooperative nodes fall into two categories: selfish nodes and malicious nodes. Selfish nodes make use of the network to send/receive packets with own interests, but refuse to forward packets for others because of the limited computation and communication resources. They do not have direct intentions to damage other nodes or the whole network.

The associate editor coordinating the review of this manuscript and approving it for publication was Kai Li.

However, the selfish nodes have great impacts on the overall network performance. In this article, we define two types of selfish nodes, namely *static selfish nodes* and *dynamic selfish nodes* (refer to Subsection IV-A). *Static selfish node* is a selfish node that remains the selfishness unchanged during the whole process, while *dynamic selfish node* varies its selfishness according to some circumstances. This article mainly analyzes the impact of *dynamic selfish node* and *static selfish nodes* comparing with normal nodes in a VANET scenario. Malicious nodes intentionally damage other nodes even the whole network while saving resources is not their primary goal. Any issues about malicious nodes are out of the scope of this article.

This article mainly focuses on quantitative analysis of the communication impact of selfish nodes in VANETs in terms of average packet delivery ratio and end-to-end delay. As described in our previous work [3], a selfish node is the node that sends/receives packets in own interests and refuses to forward packets for others in order to preserve its own resource. It is the most common passive denial of service (DoS) attack which lowers the network performance [6]. In a more precise word, the selfish nodes are not willing to forward data packets for others because of resource constrain even the control packets for routing operations. The selfish nodes in VANETs result in various harmful issues including the packet delivery ratio reduction, end-to-end delay increment, network partitioning, and much more. As clearly depicted in Fig. 1, the presence of selfish nodes causes negative implications on the network (e.g. network partitioning problem). All the related issues are discussed in detail in the following sections from various aspects.

This article is partially based on our previous conference article [3] where the impacts of selfish nodes in MANETs are studied. In this work, the selfish nodes are divided into two categories, namely static selfish nodes and dynamic selfish nodes. The dynamic selfish nodes are more close to the reality comparing with static ones. The impacts of both types of selfishness is separately investigated in VANET scenarios. The major contributions of our work are summarized as follows.

- To the best of our knowledge, this is the first work in which the node selfishness is quantitatively analyzed in VANETs scenarios in terms of the mobility, density, proportion, and combinations of selfish nodes. This work aims to cover this untouched area.
- We design a simple but typical crossroad traffic network with SUMO [7]. It is scalable for large grid networks, as a basic element of road networks.
- We classify the selfish nodes in VANETs into static and dynamic two categories. We implement the static/dynamic switching functionality at the routing table module in INET framework [8], and it is irrelevant to any routing protocol implementations. Thereby, there is no need to adjust routing protocols to test on the network with static/dynamic selfish nodes.

The remainder of this article is organized as follows: Section II presents the background of VANETs. In Section III, we discuss some recent work related to node selfishness in wireless ad hoc networks. Section IV introduces the evaluation mechanism in more detail including definition of selfish nodes, evaluation metrics, and evaluation algorithm. Simulation setup including the parameters and metrics is provided in Section V. The simulation results are discussed from various aspects in Section VI. Finally, Section VII concludes our work and points out our future research directions.

II. BACKGROUND

VANET is considered as a special type of MANETs and the key networking technology of the future ITS. The intention of VANET based ITS applications is to improve road safety, traffic efficiency and to comfort drivers and passengers on the road. The overview of the VANET architecture used in this article is illustrated in Fig. 2.

A typical VANET mainly consists of the vehicles running on the road and the RSUs fixed on the road sides [9]. The main device in the vehicle is on-board unit (OBU). OBU is usually used for collecting, exchanging, forwarding, aggregating and processing the information received from other OBUs or RSUs. The main functions of the OBU are ad hoc routing, network congestion control, wireless radio access, data transfer, security and mobility [1]. The RSU is a wave device deployed on along the road sides or special locations such as crossroads or near the parking area. The core functions of the RSU are extending the communication range by relaying information to other RSUs/OBUs, running safety applications to send various accident warnings to other RSUs/OBUs, and providing Internet connectivity to OBUs.

The VANET consists of two communication parts, namely vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. A vehicle communicates with another vehicle directly if there is a direct connection available between them. When there is no direct connection between them, a proper routing protocol is used to relay data with hop-by-hop fashion until it reaches the destination vehicle, forming the multi-hop V2V communications.

VANET has its own unique characteristics when compared with other types of wireless ad hoc networks, which include:

- *Predictable mobility:* Vehicles tend to move in an organized-fashion, because vehicles are constrained by road layout and by the traffic regulations, thereby the mobility of vehicles is predictable in some extent.
- *High dynamic topology:* Since vehicles move in relatively high speed, the topology of VANETs timely changes.
- *Hard delay constraints:* In VANET safety applications, the system always requires hard delay constraints, instead of high data rates.
- *Variable network density:* The density of VANET is more variable compared to other ad hoc networks, which could be very high in the case of traffic jam, or very low, as in suburban or rural areas.

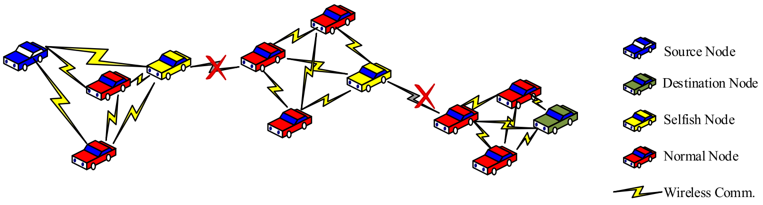


FIGURE 1. Network Partitions Caused by the Presence of Selfish Nodes in VANET.

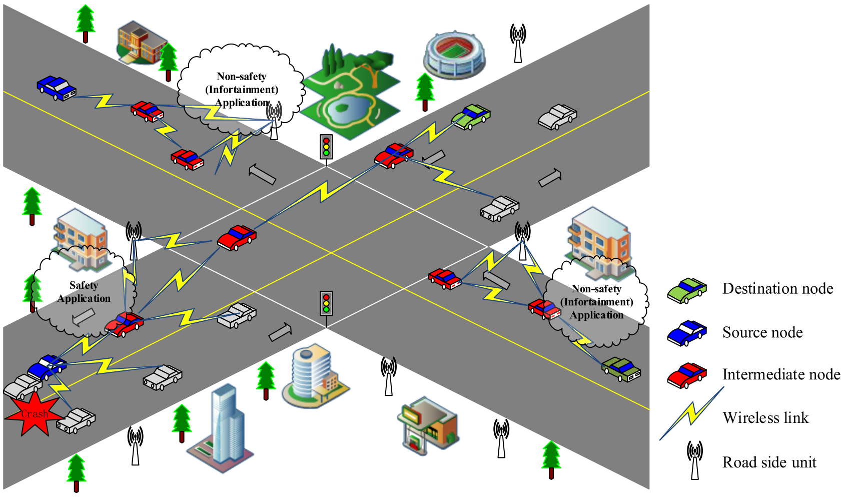


FIGURE 2. Overview of VANET Architecture.

- *Large scale network:* The number of nodes in the network could be very large in dense urban areas such as the downtown of the city.

The VANET considered in this article is a VANET only covering moving vehicles (OBUs), not including RSUs. To deploy RSUs all along roads is unfeasible considering the infrastructure costs involved in most cases.

III. RELATED WORK

In recent years, a number of researches related to node selfishness in wireless networks are extensively investigated in a various aspects. The research works done in the literature generally fall into following three categories: selfish nodes detection, incentive mechanisms for selfish nodes, and impact analysis of selfish nodes.

A. SELFISH NODE DETECTION

Selfish node detection techniques in wireless ad hoc networks are attracted by many researchers recently. Selfish behaviors are kinds of DoS attacks. Hence, all the techniques relevant to selfish node detection are also relevant to DoS attack detection. Aifa and Thomas [10] have reviewed several different selfish nodes detecting methods including Watchdog and Pathrater approaches in MANETs. Although the Watchdog approach can identify the misbehaviour nodes at the forwarding level, it is not able to detect the misbehaviour nodes in collision situations. The Pathrater approach eliminate the route containing misbehaviour nodes from the routing protocol. Vij *et al.* [11] have proposed a detection scheme for selfish nodes in MANETs which based on game theories. The proposed protocol uses the node with more resources as the intermediate forwarding node. RoselinMary *et al.* [12] have proposed an Attacked Packet Detection Algorithm (APDA) in VANETs which uses node position, velocity, and frequency, the number of packets broadcast per second, attached to road side unit (RSU) to detect DoS attacks before verification time. Singh and Sharma [13] have further developed Enhanced Attacked Packet Detection Algorithm (EAPDA) in VANETs, upgraded the algorithm by the improvement of throughput. Kim *et al.* [14] have proposed a collaborative security attack detection mechanism based on multi-class support vector machine (SVM) in software-defined vehicular cloud (SDVC) environment. However, the mechanism assumed that all vehicles in the network have sufficient resources for analyzing incoming flow data. Alrehan and Alhaidari [15] have concluded machine learning based solutions to detect distributed denial of service (DDoS) attacks on VANET systems. Khan *et al.* [16] have proposed a trust estimation scheme by employing clustering to improve cooperation among cluster members and cluster heads. In the scheme, intra-cluster and inter-cluster trust evaluation is computed independently which further reduces communication overhead and the possibility of malicious behavior in wireless sensor networks.

Furthermore, Ilavendhan and Saruladha [17] have analyzed various state-of-the-art approaches for DoS attack detection in VANETs. However, in abovementioned literature, the impact of selfish nodes, the focus of this article, is not discussed adequately in neither WANETs nor VANETs.

B. INCENTIVE MECHANISMS FOR SELFISH NODES

To reduce the harmful effects on the network caused by the presence of selfish nodes, encouraging nodes to cooperate is critical to ensure the network functioning properly. In general, incentive mechanisms can be classified into following three main kinds: reputation-based, credit-based, and barter-based system.

The main idea of reputation-based incentive mechanism is that more cooperative nodes get higher reputation scores [18]. The most challenging issue of the reputation-based incentive mechanism is to accurately measure the reputation scores to each node in the network. Wu *et al.* [19] have proposed a social norm based incentive mechanism for network coding (NC) in MANETs. A reputation system with punishment and reward is considered in the social norm. Li and Shen [20] have introduced a hierarchical account-aided reputation management system which integrates resource and price system to stimulate the node cooperation in large scale MANETs. Lai *et al.* [21] have proposed a secure incentive scheme in highway VANETs scenarios. The scheme utilizes ‘‘virtual checks’’ to ensure the security and fairness of the cooperation. The authors also developed a reputation system to stimulate cooperative nodes and penalise malicious nodes. Dias *et al.* [22] have proposed a hybrid incentive system taking advantages of both reputation mechanisms and monitoring modules in Vehicular Delay-Tolerant Networks (VDTNs). The system encourage selfish nodes to share their resources rather than excluding them from the network. Wang *et al.* [23] have investigated a blockchain based incentive content delivery in autonomous vehicular social networks. The reputation assessment models in the article is based on both social features and user behaviors. In sum, reputation-based incentive mechanisms highly rely on historical information about the node behaviors which results in the downfall of this type of incentive mechanisms.

The credit-based incentive mechanism is based on some rewarding mechanisms to the node for indicating cooperativeness [24]. Buttyán and Hubaux [25] have introduced Nuglet technique. The authors have proposed a credit-based incentive protocol that requires the node to forward each packet to its security module in MANETs. The security module, nuglet, is a counter for each node. The nuglet increases (decreases), when the node sends own (other's) packets. Meeran *et al.* [26] have proposed an enhanced selfish node detection system based on watchdog mechanism in MANETs. The system revives back selfish nodes into the network, instead of isolating them. A virtual payment (credit) is defined in the system and forwarding nodes will get credits while selfish nodes will get debited. If a node does not have enough credits, it cannot act as a source node to send packets. Zhang and Bai [27] have proposed a routing incentive mechanism based on virtual credit in VANETs. Zhu *et al.* [28] have proposed a credit-based incentive mechanism to address the problems of selfish nodes increment in VANETs. Haddadou *et al.* [29] have proposed a distributed trust model, named DTM^2, based on job market signaling model in VANETs. The model allocates ‘‘credits’’ to nodes to motivate selfish nodes to cooperate.

The barter-based strategy is also known as Tit-for-Tat (TFT) to punish uncooperative nodes. In a TFT strategy, a node takes cooperative or selfish action according to the action from previous node. Each node in the network represents a player in game theories. Hence, barter-based strategy is also considered as game theory approach. Wu *et al.* [30] have proposed a reward allocation mechanism based on the integration of game theory and reinforcement learning algorithms to maximize the whole network performance. Li and Shen [31] have integrated a reputation system and a price-based system for selfish node detection and incentives in MANETs with a game theory perspectives. Khan *et al.* [32] have introduced an evolutionary game theory based intelligent packet forwarding approach that stimulates the node cooperation in MANETs. Yang *et al.* [33] have proposed a Stackelberg game based optimal pricing strategy to model data offloading in VANETs scenarios. AI-Terri *et al.* [34] have proposed two TFT based strategies, namely Group Reputation and Cooperative Detection strategies to enforce MAC-layer cooperation in VANETs. The proposals address the greediness problem and achieve better misbehavior detection performance.

The main concern of the abovementioned incentive schemes is to stimulate or punish misbehaving nodes in the network, they did not quantitatively analyze the impact of selfish nodes on overall network performance.

C. IMPACT ANALYSIS OF SELFISH NODES

Although a wide range of investigations have done on node selfishness in various networks, very little research has been devoted to analyze the impact of node selfishness on network performance in MANETs. Xu *et al.* [5] have analyzed the effect of node selfishness in MANETs. The authors mainly consider two kinds of selfish nodes, namely type-1 and type-2. the type-1 model is the model in which the selfish nodes do not forward packets while in the type-2 model, the selfish nodes even do not take part in the routing operations. According to this work, it is obvious that the node selfishness is more harmful to network performance in the type-2 model than that in the type-1 model. Kampitaki *et al.* [35] have investigated the functions of Dynamic Source Routing (DSR) protocol, and they defined several kinds of selfish node to examine their impacts on the network performance. However, their work is lack of quantitatively analysis about node selfishness in terms of presence, mobility, and density. To the best of our knowledge, quantitative analysis of node selfishness in VANETs is still an open issue and still more work is required.

IV. EVALUATION MECHANISM

A. SELFISH NODES

Selfishness is a normal behavior that is present in all the aspects of life and the VANET is not an exception. The term ‘‘selfish node’’ appears in the work of Marti *et al.* [36]. In this article, a selfish node is a node which takes advantage of the network by sending and receiving data in own interests. However, it is unwilling to forward data for other nodes in order to preserve own resources.

We defined two types of selfish nodes in this article, namely *static selfish node* and *dynamic selfish node*. *Static selfish node* is a selfish node that remains the selfishness unchanged during the whole process, while *dynamic selfish node* varies its selfishness according to a certain probability distribution. Specifically, a uniform distribution is used in this work to determine the selfishness of a *dynamic selfish node* for the current processing packet as showing in (1). If the function returned value is equal or greater than 0.5, the node behaves as a selfish node, otherwise behaves as a normal node. However, we are more interested in *dynamic selfish nodes* than static ones, because their behaviors are more realistic.

Note that determination of a dynamic selfishness is not as simple as described in this article. In practice, it should consider all the resources the nodes keeping. The resource allocation related issues are out of scope of this article and it will be our next research direction.

$$\text{Selfishness: } \begin{cases} \mathit{selfish}, & \text{if } \mathit{uniform}(0, 1) \geq 0.5 \\ \mathit{normal}, & \text{if } \mathit{uniform}(0, 1) < 0.5 \end{cases} \tag{1}$$

Technically, the selfish node is simulated by disabling the forwarding functionality in the routing table which embedded in every node in our simulation. If it is a dynamic selfish node, the forwarding functionality switches between on (true) and off (false) according to the distribution function, whenever a packet goes through the routing table. This mechanism is independent of any routing protocols, so that testing selfish behaviors under various routing protocols is extremely simple to be conducted.

B. EVALUATION METRICS

Data forwarding is the fundamental network function in MANETs. In order to estimate the impact of node selfishness on the network performance based on packet forwarding efficiency, the following metrics are used:

1) *Average Packet Delivery Ratio (APDR)*: This metric is calculated as the division of between the number of sucessful transmitted data packets and the number of all packets sent by the source nodes.

$$APDR = \frac{\sum_{j=1}^{m} P_r(j)}{\sum_{i=1}^{n} P_s(i)} * 100\%. \tag{2}$$

In (2), n and m represent the number of transmitters and sink nodes respectively. For example, $P_s(x)$ represents the number of data packets which the node x sent. $P_r(x)$ represents the number of data packets which the node x successfully received.

2) *Average End-to-End Delay (AE2ED)*: This metric is calculated as the average sum of the difference delay of each data packet received by the sink node and the time a data packet is sent by the transmitters.

$$AE2ED = \frac{\sum_{j=1}^{m} \sum_{i=1}^{P_r(j)} [T_r^j(i) - T_s^j(i)]}{\sum_{j=1}^{m} P_r(j)}. \tag{3}$$

In (3), $T_r^i(x)$ represents the time when the i^{th} data packet received by node x, $T_s^i(x)$ represents the time when the data packet i^{th} generated by the transmitter node x.

C. EVALUATION ALGORITHM

The impact of node selfishness is examined by running a simple User Data Protocol (UDP) application on the Transport Layer [8]. The application is regarded as UDP network traffic. Every node in the network behaves as both a transmitter (sender) and a sink (receiver). Every node has a list of destination addresses in local. If the number of destination addresses is more than one, one of them is randomly chosen for each packet. The packet sending interval is $1s$ that means the packet rate is $1Pkt/s$. In this UDP application, all nodes send and receive data packets using all possible routing paths, so that the average packet delivery ratio and end-to-end delay of the network can more accurately indicate the overall network performance with avoiding the particularity of node position and mobility.

The pseudo-code of the overall application is presented in Algorithm 1 which is executed by every node in the network. At the initialization stage, all necessary variables are initialized. All incoming messages are handled by *handleMessageWhenUp* function. Self message is not normal UDP incoming message, and it is used for event scheduling. There are three kinds of self message in this application. START is the event trigger to *process_start* which is responsible for the initialization of destination addresses and socket binding. SEND is the event trigger to *process_send* which is responsible for packet sending and its pseudo-code is presented in Algorithm 2. The main tasks of *process_send* are creating application packet, randomly choose a destination address for the packet, sending the packet with the socket, and schedule next SNED event according the sending interval value. STOP is the event trigger to *process_stop* which is responsible for socket closing. The function *process_packet* is executed when UDP data packet is detected. The task of *process_packet* in this application is simply delete the received packet and increments the counter of the packet received.

The algorithm is designed by discrete event driven mechanisms. All events are scheduled by so-called self messages. There are three kinds of self messages, START, SEND, and STOP as mentioned the previous paragraph. The flow chart of the simulation algorithm is depicted in Fig. 3.

Algorithm 1 Executed by Every Node

```
initialize(int stage) // parameters initializing
repeat
    handleMessageWhenUp($msg$) // handle coming messages
until No more events available
finish() // record statistical variables
function handleMessageWhenUp($msg$)
    if is $msg$ self message then
        if $msg.kind == START$ then
            process_start()
        else if $msg.kind == SEND$ then
            process_send()
        else if $msg.kind == STOP$ then
            process_stop()
        else
            throw error
        end if
    else if is $msg$ data packet then
        process data packet
    else
        throw error
    end if
end function
```

Algorithm 2 Process Send Packets

```
$payload \leftarrow newAppPacket(name)$
$destAddr \leftarrow chooseDestAddr()$ // randomly choose one of destination addresses
socket.sendTo(payload, destAddr, destPort)
$numSent \leftarrow numSent + 1$
$t \leftarrow$ simTime() + $sendInterval$
scheduleAt(t, $msg$) // schedule next SEND self message
```

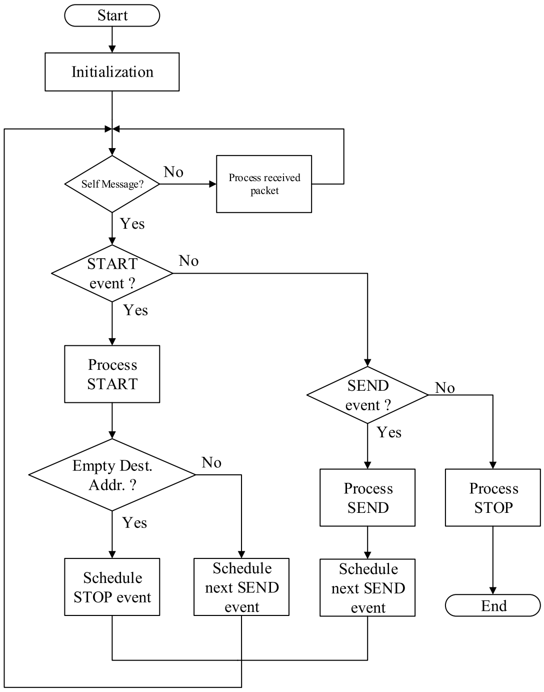


FIGURE 3. Algorithm Flow Chart.

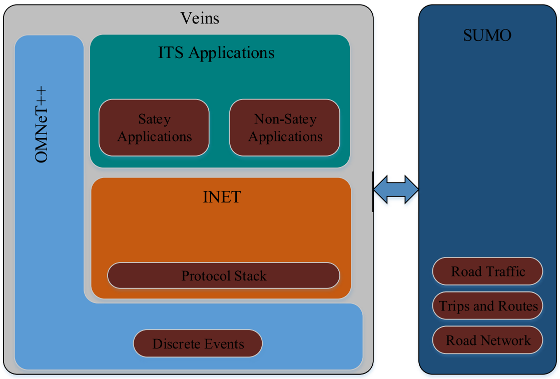


FIGURE 4. Simulation Platform.

V. SIMULATION SETUP

A. SIMULATION PLATFORM

In order to quantitatively evaluate the impact of node selfishness in VANETs, we designed the simulation procedure with using proper platforms and frameworks. The block diagram of integrated simulation platforms is given in Fig. 4.

For the purposes of our investigation, the integration of OMNeT++ (v5.5.1) [37], INET framework (v4.1.1), Eclipse SUMO (v1.2.0), and Veins (v5.0) [38] is used as the simulation platform in this article. OMNeT++ is an open source computer simulation platform written in C++ and suitable for wireless and discrete network events. INET Framework is an extension library for OMNeT++, including various protocol implementations from different network layers. Eclipse SUMO (Simulation of Urban MObility) is an open source, highly portable, microscopic and continuous multi-modal traffic simulation package designed to handle large networks. Veins is another open source framework for running vehicular simulations. It is a road traffic simulator based on OMNeT++ and SUMO to offer a comprehensive suite of models for Inter-Vehicular Communication (IVC).

For our evaluation experiments, OMNeT++ is responsible for discrete events modeling as a base of both INET framework and Veins, INET framework is responsible for communication networks providing various implementations of the network protocols, SUMO provides the road network scenario with the mobility of vehicles, and Veins is the connection between OMNeT++ and SUMO.

B. SIMULATION SCENARIO

As depicted in Fig. 5-(a), we consider a simple crossroad with traffic signals as the VANET simulation scenario, a basic pattern of road networks. The scenario is scalable to any complicated road network grid, and has adequate features that satisfy our investigation of selfishness in VANETs.

The road network scenario consists of a set of traffic signals, 18 lanes composing 3 one-way streets and 3 two-way streets, and 4 building blocks around the crossroad.

TABLE 1. Vehicle parameters.

Parameters	Values
Length	5.0m (SUMO default)
Width	1.8m (SUMO default)
Height	1.5m (SUMO default)
Acceleration	2.6m/s^2 (SUMO default)
Deceleration	4.5m/s^2 (SUMO default)
Max Speed	13.8m/s (about 50Km/h)
Min Gap	2.5m (SUMO default)
sigma	0 (denotes perfect driving)

We designed 5 circle routes in this road network on which the vehicles can move around. For simplicity, teleporting and collision are not considered in our simulation, which are not closely related to the investigation of node selfishness in this article.

As shown in Fig. 5-(b), there are 5 circle routes indicated by different colors in our VANET scenario. They are as following:

Route #1: (1)→(17)→(16)→(2)→(1);
Route #2: (12)→(17)→(11)→(7)→(12);
Route #3: (4)→(3)→(10)→(18)→(4);
Route #4: (14)→(6)→(13)→(18)→(14);
Route #5: (14)→(6)→(7)→(12)→(17)→(18)→(14).

All vehicles in the simulation are defined with the same type, and the parameters related to the vehicles are listed in Table 1. Every vehicle starts at the beginning point of its route. The vehicles are injected into the road network every 5 seconds. In another word, the injection rate of vehicles for each route is 0.2 $vehicle/s$. The VANET simulation starts, after all vehicles are injected into the road network ensuring all possible communications among vehicles on standby. In our simulation, the number of vehicles on each route is up to 8, and the start time of simulation is set to 60s. Hence, the VANET simulation starts after all vehicles are available in the network.

C. SIMULATION PARAMETERS

The general parameters of VANET simulation are listed in Table 2. Each simulation runs for 1200s. The simulation area is constrained in 200m × 1000m square area. For more realistic experimental results, the node movements follow the vehicle mobility described the previous Subsection.

In this article, according to the current standards IEEE 802.11p [39], transmission range and bit rate parameters are set as 1000m and 6$Mbps$ respectively. Ad-hoc On-Demand Distance Vector Routing (AODV) [40] protocol is used in our simulations which is a broadly used reactive routing protocol in MANETs. The time to live (TTL) of AODV is start from 2 and increases with step of 2, the maximum threshold of TTL is 7.

VI. SIMULATION RESULTS

The static and dynamic node selfishness is evaluated by our simulation platform in terms of mobility, density, proportion, and combination. Each simulation is executed 50 times and the average values are plotted with the error bars indicating 95% confidence intervals.

TABLE 2. Simulation scenarios parameters.

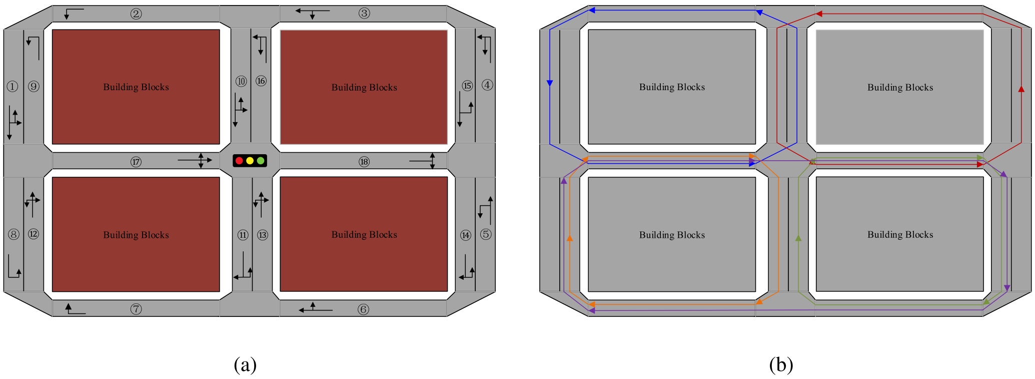
Parameters	Values
Simulation Time	1200s
Simulation Area	200m x 1000m
Number of Vehicles	up to 40
Transmission Range	1000m
Mobility	Stationary, Vehicular Mobility
Node Speed	0m/s to 13.8m/s
Packet Size	100 bytes
Packet Rate	1Pkt/s
Routing Protocol	AODV
AODV TTL	2-7 (step of 2)
Bit Rate	6Mbps
NIC	IEEE 802.11p
Radio Propagation Model	Constant Speed Propagation
Radio Path Loss Type	Nakagami Fading

A. IMPACT OF MOBILITY MODELS

One of the key characteristics of wireless ad hoc networks is mobility. For sure, mobility does affect the performance of the network. Although the investigation of various mobility models is out of this article, it is still worth to carry out some experiments to clarify the impact of mobility in VANETs. Vehicles in VANETs tend to move in an organized-fashion comparing to that in MANETs. The motion of vehicles constrained by road layout and traffic regulation (e.g. traffic signal rules), speed limit etc. In order to assess how the vehicular mobility affects the communication performance of the network with and without selfish nodes, we conduct a pertinent experiment in the VANET scenario. In the experiments, 10 vehicles are deployed in the simulation.

Two different mobility patterns are considered, namely single-route and multiple-route pattern. In single-route pattern, all vehicles run along the same single route. The route #5 (defined in Subsection V-B) is chosen randomly. All 10 vehicles run along the route round by round. In multiple-route pattern, all nodes are evenly scattered to all available routes. The average packet delivery ratio and end-to-end delay of the network are estimated under 3 different conditions which are namely *without-Selfish*, *with-Static-Selfish*, and *with-Dynamic-Selfish*. *without-Selfish*, *with-Static-Selfish*, and *with-Dynamic-Selfish* mean that all nodes are altruistic, static selfish, and dynamic selfish respectively.

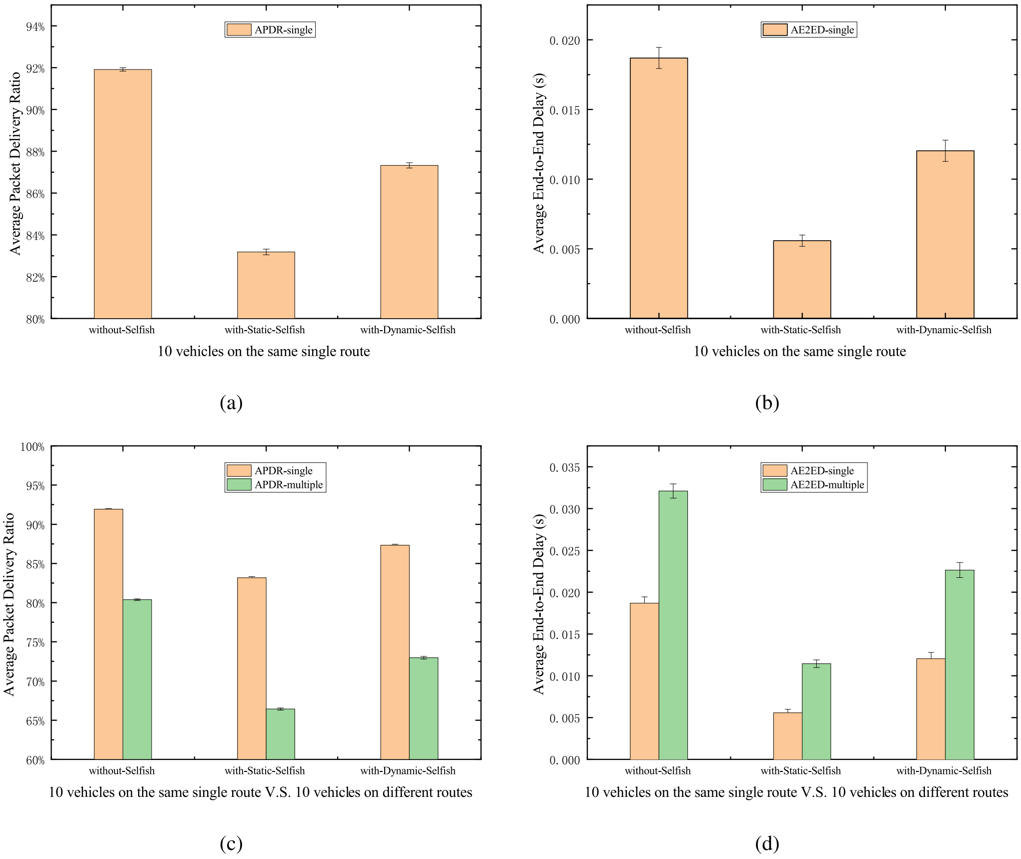
In Fig. 6-(a), the average packet delivery ratio of the network with *without-Selfish* is the highest one, because there are no selfish nodes in the network to hinder the all packets forwarding. For sure, the average packet delivery ratio of the network with *with-Static-Selfish* is the lowest one, because all the nodes in the network are static selfish which makes only direct communication, one-hop communication, is possible. The average packet delivery ratio of the network with *with-Dynamic-Selfish* is at the middle, because there is possibility that some nodes behave normally at some time to forward packets for others.



(a)

(b)

FIGURE 5. Road Network Scenario. (a) The road network. (b) The route defined in the road network.



(a)

(b)

(c)

(d)

FIGURE 6. Impact of Node Mobility. (a) The average packet delivery ratio of the network with 10 vehicles on the same single route. (b) The average end-to-end delay of the network with 10 vehicles on the same single route. (c) The average packet delivery ratio comparison between 10 vehicles on the same single route and 10 vehicles on 5 routes (2 vehicles for each route). (d) The average end-to-end delay comparison between 10 vehicles on the same single route and 10 vehicles on 5 routes (2 vehicles for each route).

In Fig. 6-(b), the average end-to-end delay of the network with *with-Static-Selfish* is the smallest one. This can be explained by (3). AE2ED is an average number that the sum of average life time of the packets successfully received by the destination node divided by the number of nodes. The number of nodes (10, in this case) is all the same under the 3 different conditions. However, the number of successfully received packets is small in the network with *with-Static-Selfish*. Another reason is that all the received packets in the network with all selfish nodes are transmitted by one-hop communication. Hence, the life time of the packets is short. This explanation also can apply to the others, *without-Selfish* and *with-Dynamic-Selfish*.

For multiple-route pattern, all 5 routes are utilized in the road network, 2 nodes for each route. The performance metrics are calculated and plotted in Fig. 6-(c,d). This simulation aims to compare the two mobility patterns in terms of average packet delivery ratio and end-to-end delay. It is obvious that average packet delivery ratio of single-route pattern is higher than that of multiple-route pattern. This is because that all nodes in single-route pattern run platoon-fashion in a single route, that results in relatively close distance between nodes. However, the end-to-end delay of multiple-route pattern is longer than that of single-route pattern. This is due to that the randomly selected destination node of some nodes is not on same route with the source node. In this case, the routing protocol spends more time to discover a valid routing path from the source node to the destination node. In single-route pattern, most packets reach their destination with one-hop communication, because they are in their transmission range.

B. IMPACT OF SELFISH NODE DENSITIES

It is reasonable to define node density as the number of nodes in the network, because the simulation area is fixed. In order to evaluate the impact of selfish nodes in various-density networks, the following experiments are conducted. All the routes defined in the road network are used in the simulation. The number of vehicles in each route increases from 1 to 8 with the step of 1. It means the total number of nodes in the network increases from 5 to 40 with the step of 5. The average packet delivery ratio and average end-to-end delay are measured in three different networks with three different types of nodes (normal, static selfish and dynamic selfish).

In the evaluation algorithm, the list of destination nodes of each node includes all nodes in the network. It implies that the destination node might be the node itself. The less nodes deployed in the network, the more likely it occurs. A packet is simply received without loss when a node sends it to itself. As depicted in Fig. 7, APDR of the network is the highest one, where there are 5 nodes in the network. This is because there are high probabilities (20%) to pick itself as the destination node. However, AE2ED of the network is the longest one, where there are 5 nodes in the network. This is due to the fact that the 5 vehicles are running on different routes and the distances between them are relatively large. With increasing node densities, the performance of the network increases in terms of average packet delivery ratios. The main reason is that there are more and more nodes on the same route which results in higher node density on the route and the crossroad where the routing protocol easily discover a valid routing path from the source node to the destination. The performance of the network with dynamic selfish nodes is about the average performance of the other two networks. This is because of the dynamic selfish node with the 50% probabilities to be selfish or altruistic to forward each packet.

To sum up, higher node densities produce more chances to build routing path between source nodes and destination nodes. The dynamic selfish nodes play negative roles in the network and the static ones play more worse.

C. IMPACT OF SELFISH NODE PROPORTION

Selfish nodes play negative roles in VANETs as intermediate nodes which refuse to forward packets for others' interests. The multi-hops communication is required in VANETs, whenever a node sends a packet to the destination who is out of its transmission range of the node. It points out that cooperation among nodes in VANETs is indispensable in most cases. For the estimation of impacts of selfish nodes proportion in a VANET, the following experiments are carried out.

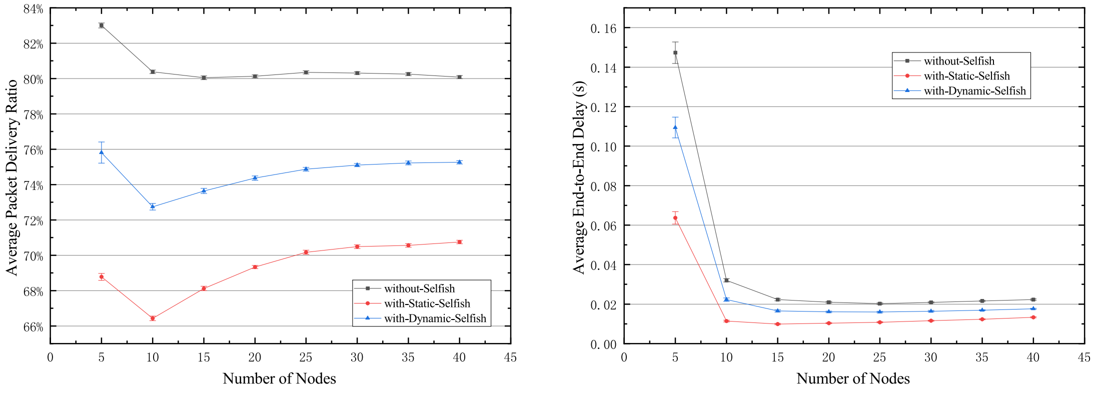
The average packet delivery ratio and end-to-end delay are investigated in the VANET scenario which consists of 40 vehicles. The simulations with static selfish nodes and dynamic selfish nodes are carried out separately. The selfish nodes are randomly selected at the configuration stage before the simulation started. In fact, the different combinations of selfish nodes have different levels of impacts on the network performance. It will discussed in Subsection VI-D in more detail. The proportion of selfish nodes ranges from 0% to 100% with the increments of 10%.

The experimental results are shown in Fig. 8. Both APDR and AE2ED significantly decrease in both types of networks. In the network with *with-Static-Selfish* nodes, the APDR decreases from 80.1% to 70.7% while the AE2ED decreases from 0.222s to 0.133s. In the network with *with-Dynamic-Selfish* nodes, the APDR decreases from 80.1% to 75.3% while the AE2ED decreases from 0.222s to 0.017s. The reduction of APDR means the decrement of network performance. However, the reduction of AE2ED does not really mean the decrement of network performance. The reason can be explained by the explanation in Subsection VI-A. As a result, the node selfishness has great impacts to worse the network performance in terms of packet delivery ratio and end-to-end delay in VANETs. Undoubtedly, because of lack of packet forwarding, the more selfish nodes are, the worse performance is.

D. IMPACT OF VARIOUS COMBINATIONS OF SELFISH NODES

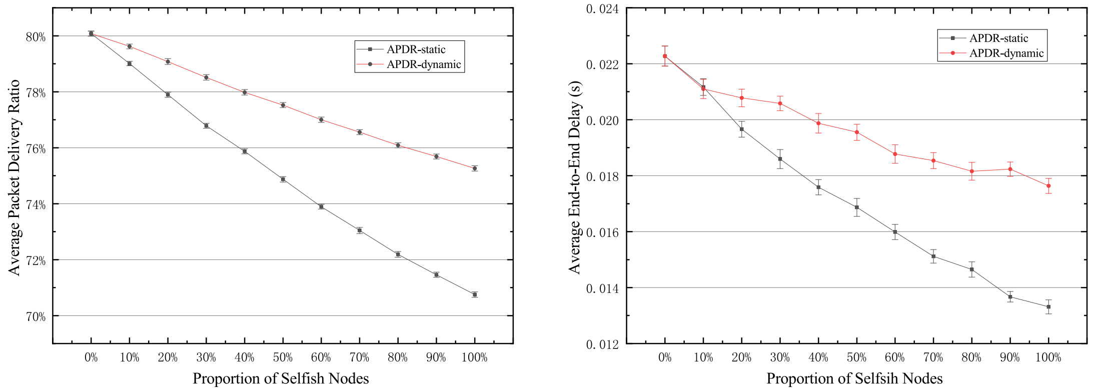
The combination of selfish nodes is one of unnegligible factors to evaluate the node selfishness in a VANET. Every individual vehicle in VANETs has different positions, speeds, and neighbors. Furthermore, these are also time-varying due to the dynamic mobility. Generally speaking, different selection of selfish nodes affect the network performance differently. In fact, the evaluation of various combinations of selfish nodes integrates the impacts of mobility, speed, and positions in VANETs.

For the purpose of evaluation about the various combination of selfish nodes, following simulations are conducted. There are 5 vehicles running on the same route (#5), and 2 of them are selfish nodes. It means that 40% of nodes are selfish. There are 10 possible combinations, i.e. (0,1), (0,2), (0,3), (0,4), (1,2), (1,3), (1,4), (2,3), (2,4), and (3,4). The experimental results are given in Fig. 9. The (i, j) denotes that



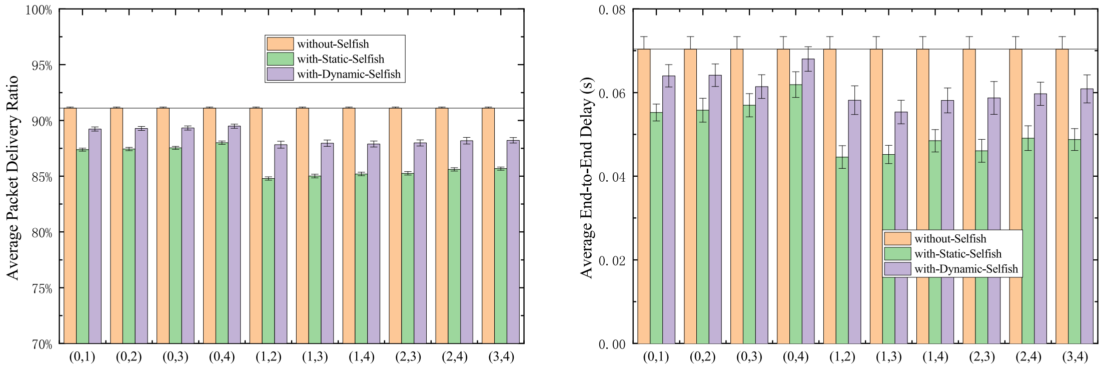
(a) (b)

FIGURE 7. Impact of Selfish Node Densities. (a) The average packet delivery ratio of the network with varying number of nodes. (b) The average end-to-end delay of the network with varying number of nodes.



(a) (b)

FIGURE 8. Impact of Node Proportion. (a) The average packet delivery ratio of the network with different proportions of selfish nodes. (b) The average end-to-end delay of the network with different proportions of selfish nodes.



(a) (b)

FIGURE 9. Impact of Node Combinations. (a) The average packet delivery ratio of the network with different combinations of selfish nodes. (b) The average end-to-end delay of the network with different combinations of selfish nodes.

the nodes indexed i and j are selfish nodes. From Fig. 9-(a), we can observe that different combinations of selfish nodes produce different packet delivery ratios, even the same type of selfishness. For example, in the network with *with-Static-Selfish*, the APDR falls down to the lowest value, 84.7%, when *node*(1) and *node*(2) are selfish. However, it reaches the highest value, 87.9%, when *node*(0) and *node*(4) are selfish. In Fig. 9-(b), it is also clear that different combinations of selfish nodes have different levels of impacts on average end-to-end delays in the network. For instance, in the network with *with-Static-Selfish*, the longest AE2ED is $0.062s$, when *node*(0) and *node*(4) are selfish. However, the shortest AE2ED is $0.044s$, when *node*(0) and *node*(4) are selfish. Note that the APDR and AE2ED of the network with *without-Selfish* nodes are plotted as well in the figure as a reference line making comparison clear.

In a word, the different selections of selfish nodes have different extents of impacts on the performance of VANETs. Moreover, all the analyses of in this subsection also could explain the impacts caused by node positions and velocities.

VII. CONCLUSION AND FUTURE WORK

Based on our investigations, there are significant impacts of selfish nodes in VANETs in terms of average packet delivery and end-to-end delay, no matter what kind of selfishness. In general, the more selfish nodes are, the worse the network performance is in VANETs. Static selfish nodes are more harmful than dynamic ones, because more packets are refused by static selfish nodes. However, dynamic selfishness is more close to the reality than static one. It is crucial to make clear the reasons of selfishness, because it is the base of selfish node detection mechanisms. For future work, we are interested in more effective selfish node detection and incentive mechanisms based on resource allocation in VANET scenarios.

REFERENCES

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[2] R. Iqbal, T. A. Butt, M. O. Shafiq, M. W. A. Talib, and T. Umar, "Context-aware data-driven intelligent framework for fog infrastructures in Internet of vehicles," *IEEE Access*, vol. 6, pp. 58182–58194, 2018.

[3] A. Shan, X. Fan, and X. Zhang, "Quantitative study on impact of node selfishness on performance of MANETs," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Beijing, China, Aug. 2020, pp. 9–14.

[4] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Veh. Technol. Mag.*, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[5] L. Xu, Z. Lin, and A. Ye, "Analysis and countermeasure of selfish node problem in mobile ad hoc network," in *Proc. 10th Int. Conf. Comput. Supported Cooperat. Work Design*, Nanjing, China, May 2006, pp. 1–4.

[6] H. Yadav and H. K. Pati, "A survey on selfish node detection in MANET," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Greater Noida, India, Oct. 2018, pp. 217–221.

[7] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner, "Microscopic traffic simulation using SUMO," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 2575–2582.

[8] INET Framework Development Team. *Inet Framework*. Accessed: Oct. 10, 2020. [Online]. Available: https://inet.omnetpp.org/

[9] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, and A. Ksentini, "Named data networking in vehicular ad hoc networks: State-of-the-art and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 320–351, 1st Quart., 2020.

[10] S. Aifa and T. Thomas, "Review on different techniques used in selfish node detection," in *Proc. Int. Conf. Circuits Syst. Digit. Enterprise Technol. (ICCSDET)*, Kottayam, India, Dec. 2018, pp. 1–4.

[11] A. Vij, V. Sharma, and P. Nand, "Selfish node detection using game theory in MANET," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Greater Noida, India, Oct. 2018, pp. 104–109.

[12] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using attacked packet detection algorithm (APDA)," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Chennai, India, Feb. 2013, pp. 237–240.

[13] A. Singh and P. Sharma, "A novel mechanism for detecting DOS attack in VANET using enhanced attacked packet detection algorithm (EAPDA)," in *Proc. 2nd Int. Conf. Recent Adv. Eng. Comput. Sci. (RAECS)*, Chandigarh, India, Dec. 2015, pp. 1–5.

[14] M. Kim, I. Jang, S. Choo, J. Koo, and S. Pack, "Collaborative security attack detection in software-defined vehicular networks," in *Proc. 19th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Seoul, South Korea, Sep. 2017, pp. 19–24.

[15] A. M. Alrehan and F. A. Alhaidari, "Machine learning techniques to detect DDoS attacks on VANET system: A survey," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Riyadh, Saudi Arabia, May 2019, pp. 1–6.

[16] T. Khan, K. Singh, L. H. Son, M. Abdel-Basset, H. V. Long, S. P. Singh, and M. Manjul, "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks," *IEEE Access*, vol. 7, pp. 58221–58240, 2019.

[17] A. Ilavendhan and K. Saruladha, "Comparative analysis of various approaches for DoS attack detection in VANETs," in *Proc. Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Coimbatore, India, Jul. 2020, pp. 821–825.

[18] G.-U. Rehman, A. Ghani, M. Zubair, S. H. A. Naqvi, D. Singh, and S. Muhammad, "IPS: Incentive and punishment scheme for omitting selfishness in the Internet of vehicles (Iov)," *IEEE Access*, vol. 7, pp. 109026–109037, 2019.

[19] C. Wu, M. Gerla, and M. van der Schaar, "Social norm incentives for network coding in manets," *IEEE/ACM Trans. Netw.*, vol. 25, no. 3, pp. 1761–1774, Jun. 2017.

[20] Z. Li and H. Shen, "A hierarchical account-aided reputation management system for large-scale MANETs," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 909–917.

[21] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1559–1574, Jun. 2017.

[22] J. A. F. F. Dias, J. J. P. C. Rodrigues, N. Kumar, and C. X. Mavromoustakis, "A hybrid system to stimulate selfish nodes to cooperate in vehicular delay-tolerant networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 5910–5915.

[23] Y. Wang, Z. Su, K. Zhang, and A. Benslimane, "Challenges and solutions in autonomous driving: A blockchain approach," *IEEE Netw.*, vol. 34, no. 4, pp. 218–226, Jul. 2020.

[24] M. Kou, Y. Zhao, H. Cai, and X. Fan, "Study of a routing algorithm of Internet of vehicles based on selfishness," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Xi'an, China, Aug. 2018, pp. 34–39.

[25] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579–592, 2003.

[26] A. Meeran, N. A. Praveen, and K. T. Ratheesh, "Enhanced system for selfish node revival based on watchdog mechanism," in *Proc. Int. Conf. Trends Electron. Informat. (ICEI)*, May 2017, pp. 332–337.

[27] X. Zhang and X. Bai, "Research on routing incentive strategy based on virtual credit in VANET," in *Proc. 20th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Matsue, Japan, Sep. 2019, pp. 1–4.

[28] Y. Zhu, L. Liu, J. Panneerselvam, L. Wang, and Z. Li, "Credit-based incentives in vehicular ad hoc networks," in *Proc. IEEE 8th Int. Symp. Service Oriented Syst. Eng.*, Oxford, U.K., Apr. 2014, pp. 352–357.

[29] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3657–3674, Aug. 2015.

[30] C. Wu, T. Yoshinaga, Y. Ji, and Y. Zhang, "Computational intelligence inspired data delivery for vehicle-to-roadside communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12038–12048, Dec. 2018.

[31] Z. Li and H. Shen, "Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 8, pp. 1287–1303, Aug. 2012.

[32] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile adhoc networks," *IEEE Access*, vol. 8, pp. 124097–124109, 2020.

[33] F. Yang, J. Yan, Y. Guo, and X. Luo, "Stackelberg-game-based mechanism for opportunistic data offloading using moving vehicles," *IEEE Access*, vol. 7, pp. 166435–166450, 2019.

[34] D. Al-Terri, H. Otrok, H. Barada, M. Al-Qutayri, and Y. Al Hammadi, "Cooperative based tit-for-tat strategies to retaliate against greedy behavior in VANETs," *Comput. Commun.*, vol. 104, pp. 108–118, May 2017.

[35] D. G. Kampitaki, E. D. Karapistoli, and A. A. Economides, "Evaluating selfishness impact on MANETs," in *Proc. Int. Conf. Telecommun. Multimedia (TEMU)*, Heraklion, Greece, Jul. 2014, pp. 64–68.

[36] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Boston, MA, USA, 2000, pp. 255–265.

[37] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proc. 1st Int. Conf. Simulation Tools Techn. Commun., Netw. Syst. Workshops (Simutools)*. Brussels, Belgium: Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2008, p. 60.

[38] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3–15, Jan. 2011.

[39] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2016 (Revision of IEEE Std 802.11-2012), 2016, pp. 1–3534.

[40] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl. (WMCSA)*, Feb. 1999, pp. 90–100.

AXIDA SHAN (Graduate Student Member, IEEE) received the B.S. degree in computer networking from Inner Mongolia University, Hohhot, China, in 2004, and the M.S. degree in information network system from The University of Electro-Communications, Tokyo, Japan, in 2010. He is currently pursuing the Ph.D. degree with the Department of Automation and Information Engineering, Xi'an University of Technology, Xi'an, China. He is currently a Faculty Member with the Baotou Teachers' College, Baotou, China. His research interests include high-performance computing, the Internet of Things, vehicular computing, ad hoc networks, and incentive mechanisms for cooperative computing.

XIUMEI FAN (Member, IEEE) received the bachelor's degree from Tianjin University, China, in 1989, and the Ph.D. degree Beijing Jiaotong University, China, in 2002. She was a Professor with the Beijing Institute of Technology from 2004 to 2013. She is currently a Professor with the Xi'an University of Technology and the Shaanxi Province Hundred Talents Program. Her main research interests include vehicular networks, the mobile internet, edge computing, and various aspects of broadband wireless networks.

CELIMUGE WU (Senior Member, IEEE) received the Ph.D. degree from The University of Electro-Communications, Japan, in 2010. He is currently an Associate Professor with the Graduate School of Informatics and Engineering, The University of Electro-Communications. His current research interests include vehicular networks, the IoT, big data, and mobile edge computing. He is/has been the TPC Co-Chair of the Wireless Days 2021, Wireless Days 2019, ICT-DM 2019, and ICT-DM 2018, and the Track Co-Chair of many international conferences, including the ICCCN 2019 and IEEE PIMRC 2016. He is the Chair of the IEEE TCGCC SIG on Green Internet of Vehicles and the IEEE TCBD SIG on Big Data with Computational Intelligence. He is serving as an Associate Editor for the IEEE Transactions on Network Science and Engineering, the IEEE Transactions on Green Communications and Networking, IEEE Access, *Wireless Networks*, the *IEICE Transactions on Communications*, the *International Journal of Distributed Sensor Networks*, and *MDPI Sensors*. He is/has been a Guest Editor of the IEEE Transaction on Intelligent Transportation Systems, IEEE Transactions on Emerging Topics in Computational Intelligence, the *IEEE Computational Intelligence Magazine*, and ACM/Springer MONET.

XINGHUI ZHANG received the B.S. degree from the Liaoning University of Technology, China, in 2004, and the M.S. degree from the Changchun University of Science and Technology, China, in 2009. He is currently pursuing the Ph.D. degree with the Xi'an University of Technology. He was a Lecturer with Ankang University from 2009 to 2018. His main research interests include data prediction and various aspects of intelligent transportation.