IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 12, 2019, accepted July 27, 2019, date of publication August 8, 2019, date of current version August 21, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2933873*

# IPS: Incentive and Punishment Scheme for Omitting Selfishness in the Internet of Vehicles (Iov)

**GHANI-UR-REHMAN[1,2], ANWAR GHANI[1], MUHAMMAD ZUBAIR[2], SYED HUSNAIN A. NAQVI[1], DHANANJAY SINGH[3], (Senior Member, IEEE), AND SHAD MUHAMMAD[2]**

[1]Department of Computer Science and Software Engineering, International Islamic University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Science and Bioinformatics, Khushal Khan Khattak University, Karak 27000, Pakistan
[3]Department of Electronics Engineering, Hankuk University of Foreign Studies, Yongin 17035, South Korea

Corresponding author: Dhananjay Singh (dan.usn@ieee.org)

This work was supported by the Hankuk University of Foreign Studies Research Fund 2019.

**ABSTRACT** Internet of Vehicles (IoV) is a new emerging concept and is an extended notion of Vehicular Ad-hoc networks (VANETs). In IoV the vehicles (nodes) are connected to the internet and able to transmit information. However, due to resources constraint nature of vehicles, they may not want to cooperate in order to save its own resources such as memory, energy, and buffer, etc. This behavior may lead to poor system performance. IoV needs an efficient solution to motivate the nodes in terms of cooperation to avoid selfish behavior. A novel mechanism Incentive and Punishment Scheme (IPS) has been proposed in this article where vehicles with higher weight and cooperation are elected as Heads during the election process. Vickrey, Clarke, and Groves (VCG) model has been used to scrutinize the weight of these heads. Vehicle participating in the election process can increase its incentives (reputation) by active participation (forwarding data). Vehicles with repeated selfish behavior are punished. The monitoring nodes monitor the performance of their neighbor nodes after the election process. A mathematical model and algorithms has been developed for the election, monitoring and incentive processes. The proposed approach has been simulated through VDTNSim environment to analyze the performance of the proposed IPS. The performance results demonstrate that the proposed schemes outperform the existing schemes in terms of packet delivery ratio, average delivery delay, average cost, and overhead.

**INDEX TERMS** Internet of vehicles, smart objects, VCG model, selfish behavior, incentive techniques.

## I. INTRODUCTION

Social economy has improved the living standard of human life in recent years. The increase in the number of vehicles has increased the number of accidents, especially in urban traffic. To minimize the number of accidents in urban traffic and to ensure human safety while traveling, a new field of a vehicular ad-hoc network (VANET) has emerged called Internet of Vehicles (IoV) [1]. IoV is another form of the internet of things (IoT) in which vehicle is connected to the internet these days. The road problems like traffic congestion and road accident can be solved by IoV. It is mainly used in the automobile industry, traffic management and can be used in smart cities applications. IoT connects the smart objects to communicate with each other to make a global network [2]. The smart objects in the IoV are the parked and moving vehicles that make IoT as IoV [3], [4]. It is the extension of the IoT in intelligent transportation applications.

The IoV has been proposed to sense the data and process it for smart transport system [5], [6]. It consists of parked and moving vehicles, roads side units (RSUs), traffic lights and handheld devices used by the passengers and the general public [7]. The nodes participating in the IoV have single ownership, person or organization [8], [9]. Nodes, however, exhibit selfish behavior by preserving its own resources and using an external one. Cooperation of the nodes in IoV is very critical as it affects the performance of the network and overall system. The nodes in the network are divided into

The associate editor coordinating the review of this article and approving it for publication was Nafees Mansoor.

normal and abnormal nodes [10]. Normal nodes vigorously transmit data to its neighbors and show cooperation whereas the abnormal nodes usually degrade the network performance due to the lack of active participation. Selfish nature of a node is due to certain reasons such as limited resources, energy saving, bandwidth preservation, manipulation, self-centered and many other social aspects [11].

Different techniques for example cooperative watchdog system and multi-heads clustering have been proposed to encourage nodes for cooperation in the network. The first scheme encourages the nodes cooperation based on reputation score. While the second scheme motivates nodes for cooperation based on weight. The cluster heads are elected in the election also based on weight. However, these two techniques have drawbacks such as (i) the monitoring nodes or watchdogs are handled equally, that can lead to inaccurate results (ii) No warning is given to selfish node by showing selfish behavior for the first time [12] (iii) weight tie problem: when two node have the same weights for heads nomination during the election process, in such case no alternate requirement is defined [13]. The proposed election criteria to omit selfishness is different from these techniques in different ways like the issue of weight tie has been solved where nodes have the same weights for heads nomination during the election process by adding cooperation as the next criteria. Also, the monitoring nodes are treated differently that leads to reliable results and nodes are given warning for showing selfish behavior for the first time.

In this article an incentive and punishment scheme (IPS) has been proposed. This scheme motivates the nodes to participate in the network activities. The motivation is also vital as the IoV has less availability of the roadside units and other smart objects. In a single cluster, the participating nodes move in the same direction that makes the monitoring system more active. Election process is used to elect Cluster Head (CH), Auxiliary Cluster Head (ACH) and Incentive Head (IH) for each cluster. The nodes participating in the election process belong to one cluster to elect cluster head inside the cluster. The election is based on the weight, cooperation, and a number of votes to elect these heads. The node with higher weight, cooperation, and a number of votes is elected as CH. Node with second and third highest votes will be elected as ACH and IH respectively.

Behavior of the nodes are monitored constantly by monitoring nodes selected by the CH, ACH, and IH. The selfish nodes are punished for showing selfish behavior. Similarly, some incentives or payment is awarded to the cooperative nodes in the form of reputation. The IPS is used in IoV and encourages the selfish nodes to cooperate with one another based on social technique. This scheme helps in omitting selfishness in the network through punishment strategies and encourages cooperative behavior through incentives.

The main contributions of the proposed scheme in IoV are;

- To analyze the behavior of nodes in IoV and determine whether the nodes behave selfishly?
- To analyze the impact of the node's behavior on the performance of the network and to design an approach that stimulate the selfish nodes for cooperation. In order to improve the overall performance of the system based on node weight having mobility parameters and node energy to elect different heads for example, CH, ACH, and IH.
- To design a technique for solving weight tie among nodes for heads nomination during election process by adding cooperation as criteria for the nomination of heads in election. It has also a monitoring system where monitoring nodes are selected by the three heads that constantly monitor the behavior of nodes based on Joined Importance Factor (JIF).
- A comparative analysis has been presented to compare the proposed approach with existing incentive based techniques. Furthermore, the proposed approach has improved the network performance in term of packet delivery ratio, average delivery delay, average cost and overhead.

The remainder of the paper is organized as follows: Related work is discussed in Section II. The detailed design of IPS is presented in Section III, which include the system model and some discussions. The performance evaluation of IPS is presented in Section IV. Section V concludes the paper.

## II. RELATED WORKS

IoV has certain nodes which are selfish in nature. This has gained a lot of attention from the researchers. The impact of selfish nodes has been extensively explored. The selfish nodes degrade the performance of the network [14]. Incentive-based schemes are adapted to stimulate the node with selfish behavior to cooperate and share its resources [15]. The incentive mechanism is divided into four categories reputation based, credit-based, game-theoretic and barter-based system.

The reputation-based incentive mechanism is based on the degree of cooperation of the nodes in the network. Cooperative nodes are highly valued compared to the non-cooperative nodes. The reputation score is assigned to the nodes in the Cooperative Watchdog System (CWS) [13]. The connecting nodes share information about their resources and behaviors in a network. Participated nodes score is updated by the CWS based mechanism. Usually, some kind of score is assigned to it. The issue of selfishness in Vehicle Delay Tolerant Network is addressed in Dias *et al.* [16]. This mechanism calculates the score of the nodes upon delivery of successful data to another node. The score is increased by a certain number upon successful delivery of packets; otherwise, the score is decreased by a certain number. Kou *et al.* [17] proposed an incentive cooperation model to encourage the selfish nodes to cooperate in the network. Wei *et al.* [18] proposed a reputation based incentive system for Opportunistic network called Community and Reputation-based Incentive Scheme for Opportunistic Networks (CARISON). It has two types of nodes in the community, namely: supernodes and ordinary nodes. The reputation is two ways: inter-communities and intra-communities based on their capacities.

The credit-based system works on giving away some rewards to the nodes for showing cooperation. This rewarded credit can be used by the nodes for its own purpose later. Zhang and Wu [19] has proposed an incentive scheme for Vehicular ad-hoc network. Bargaining game approach is followed in the scheme to motivate the selfish nodes to share its information with other participating nodes. Ning *et al.* [20] uses virtual credit as an incentive to encourage the nodes to share its information with other nodes in a network. Copy Adjustable Incentive Scheme (CAIS) divides the nodes into different communities based on their relationship with other nodes. Jedari *et al.* [21] discussed the problem of some socially selfish nodes. The proposed scheme called Game-Theoretic Incentive Scheme for Social-aware routing (GISS) that works on four components social utility calculators, message handler, incentive scheme, and selfish aware message delivery.

Barter-based incentive mechanisms, also called Tit-For-Tat (TFT) strategy, in which nodes share the same amount of information. Zhou *et al.* [22] uses pair-wise Tit-For-Tat (TFT) technique. It uses incentive driven and Publisher/Subscribe approach to deal with selfish nodes in the network. Buttyan *et al.* [23] uses the barter system to trade the message with other nodes in the network. This approach is also called give one and get one approach. Another barter approach is discussed in Liu *et al.* [24], this system barter between nodes and communities for message forwarding. The messages are barter traded between node and community. Umar *et al.* [25] has proposed a game theoretic reward based technique which reduced a load of nodes in the network by encouraging them to behave in a cooperative manner. This social aspect of the nodes is utilized by the researchers to tackle the routing and other issues like social selfishness in a network. SSAR [26] is one of the approaches to omit social selfishness in a network. In a social community, the nodes having a strong social relationship are likely willing to forward messages to one another in a network. Liu *et al.* [27] uses an incentive scheme to share nodes information in the vehicular social network. The information shared is related to road accidents, construction of roads, and traffic delays. Jesudoss *et al.* [28] proposed a payment and punishment strategy to encourage nodes for telling truth and cooperation. Fawaz [29] discussed the non-cooperative vehicles on path connectivity in vehicle networks by using Unmanned Aerial Vehicles (UAVs) as store-carry-and-forward nodes in a Network. Li and Wang [30] proposed two-phase-based generous cooperative routing protocol for omitting selfishness in Vehicle to Vehicle networks. Socievole *et al.* [31] proposed a social based scheme to discourage selfish behavior and motivate the nodes for data forwarding. De Rango *et al.* [32] proposed a Multi-layer Social based routing which gets social information from nodes to perform routing decision. Socievole et al. [33] improve the data forwarding in social opportunistic networks by getting information from both offline and online users. Socievole et al. [34] tackled the issue of selfishness in opportunistic networks. Trust is also considered one of the important components in cooperative communication. Vamsi et al. [35] proposed BT-AODV scheme to detect selfish nodes in the routing process. Venkana et al. [36] proposed a scheme called Trust and energy based AODV to handle the issue of selfishness. In the proposed scheme, they have selected the cooperative routes instead of shortest available paths to isolate the selfish nodes.

## III. INCENTIVE AND PUNISHMENT SCHEME

The proposed scheme focuses mainly on the participation of the node in the network. The nodes in the network participate in different activities related to the network performance like message forwarding and monitoring of other nodes in a network. These activities are considered to be the key responsibilities of the nodes in the process of election. The nodes are motivated to participate in the network when the nodes work as a unit and coordinate with each other. Monitoring of the fellow node's behavior in terms of sending and receiving of the message is found more in clustered-based message forwarding. This feature of a node gives control over the message forwarding and receiving. Hence, the proposed scheme suggests an incentive or payment in the form of reputation to stimulate and motivate the nodes to perform its functions in the network. The proposed IPS scheme makes payment to the nodes for (i) for active participation in the election process (ii) to forward data to the neighbor nodes (iii) to monitor the behavior of the nodes. These three are explained below in subsections. On the other hand, nodes having selfish behavior are encouraged to participate in the election process and behave as cooperative nodes. In case of repeatedly showing selfish behavior, the selfish nodes are punished in the form of expulsion from the cluster and broadcast this message within the cluster about these nodes. The centralized authority decides the three system parameters like the per-node budget, relay node payment, and monitoring nodes payment during the registration process of nodes in IoV. The overall system model has been presented in the FIGURE 1.

### A. INCENTIVE FOR ELECTION PARTICIPATION

The proposed scheme IPS forward data in the cluster. The process begins with nodes participation in the election process. The cluster formation and maintenance process is out of scope for this paper and hence is not discussed here.

#### 1) ELECTION PROCESS

The cluster is managed by election process periodically. The election is based on the eligibility criteria. For eligibility, two characteristics of nodes are checked such as weight and cooperation. Nodes with higher (remaining) weight and cooperation in the cluster are nominated for election. The weight is actually the number of resources a node possessed. The weight of any node is measured by a number of neighbors, relative position, energy, buffer and speed to the mean position.

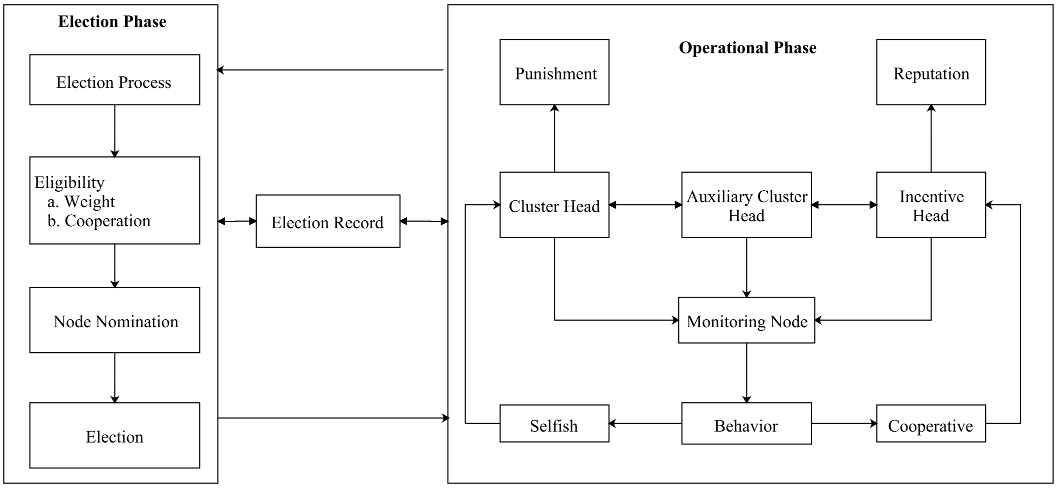


**FIGURE 1.** Overall model of the proposed approach.

The node with the highest score (weight, cooperation, and votes) becomes the cluster head $CH$. Second highest weight scorer will become $ACH$ and the node with the third highest scorer will become $IH$. To ensure the stability of the cluster the $ACH$ will become $CH$ if the $CH$ moves away from the cluster and is lost. Every cluster head $CH$ has unique Cluster-id. The $CH$ uses MAC-id to generate unique cluster-id after every election process. The cluster-id generated by the $CH$ is maintained by the succeeding $ACH$ until both heads vanished at the same time. The incentive head $IH$ makes payment as an incentive to the cooperative nodes in the network. All these three elected heads collectively select some monitoring heads that monitor the behavior of the nodes in each cluster. The calculation of node weight is explained as follow:

Relative Distance ($RD_m$): By [12] the vehicles in the cluster have a certain property of how close they are to each other. Each vehicle calculates its own closeness to the mean distance and is given by the following formula:

$$RD_m = \mid m_{pos} - \omega_{pos} \mid = \sqrt{((X_m - X_\omega)^2 + (Y_m - Y_\omega)^2)} \quad (1)$$

In the above equation, $m_{pos}$ shows the position of $m$, the mean position of any node with its neighbors of $m$ is represented by $\omega_{pos}$, $(X_m, Y_m)$ is the $X$ and $Y$ coordinates of node $m$ and $(X_\omega, Y_\omega)$, shows the coordinate of $\omega$ position.

Relative Speed ($RS_m$): Vehicle in the cluster can have different speeds. It is assumed that the two vehicles will travel for longer if their relative speed is closer to each other. $m_{speed}$ being speed of any node $m$ and $\omega_{speed}$ being speed of its neighbor vehicles, thus the relative speed can be calculated as:

$$RS_m = \mid m_{speed} - \omega_{speed} \mid \quad (2)$$

Node Degree $ND_m$: This shows the number of nodes as neighbor nodes contained in the range of transmission of a node $m$.

$$ND_m = \sum_{l \in n, l \neq m} \{ l \mid dis(m, l) < T_{range} \} \quad (3)$$

Energy$E_m$: The nodes in IoV have limited resources. So energy is also limited. Let $E_m$ be the remaining energy and is given by:

$$E_m = \frac{Er_m}{Emax_m} \times 100\% \quad (4)$$

where, $Er_m$ is the remaining energy of node $m$ currently and $Emax_m$ is the maximum energy of node $m$.

Buffer($B_m$): Saving more data to buffer actually reduces space in the buffer. Where $B_m$ is the percentage of buffer remaining which represents the node status in the form of buffer. The remaining buffer is given by:

$$B_m = \frac{Br_m}{Bmax_m} \times 100\% \quad (5)$$

where $Br_m$ is the remaining buffer of node $m$ currently and $Bmax_m$ is the maximum buffer. Once the values of all five attributes are calculated, then its weight is given by:

$$W_m = RD_m.wt_1 + RS_m.wt_2 + ND_m.wt_3 + E_m.wt_4 + B_m.wt_5 \quad (6)$$

where $W_m$ is the weight of a node $m$, the weights $(wt_1, wt_2, wt_3, wt_4, wt_5)$ are selected randomly, where the total weight is equal to 1 similar to [37]. If the weight of two nodes is found to be same then the cooperation is considered as the nomination criteria. The cooperation of a node is given by:

$$cp_m = \sum_{n \in N} Rc_m(n), \ if \ cp_m > k \quad (7)$$

where $k = \lceil \frac{n}{3} \rceil$, $cp_m$ is the cooperation of node $m$, $n$ is all nodes in the cluster and $Rc_m$ is the total number of contacts of node $m$. The nodes having contacts with the majority of other nodes in the cluster i.e. $cp_m > k$ are considered as a cooperative one. For measuring the selfishness, the nodes having contacts $cp_m \leq k$ are considered as a selfish one. Nodes can contact one another in its communication range for a short period of time. The detail of the election process and incentive payment is presented in Algorithm 1.

**Algorithm 1** Election Process and Incentive Payment Algorithm

**Require:** Number of nodes $n$
**Ensure:** Heads election & Payment during Election
**for** $m = 1 : n$ **do**
  Compute and broadcast $W_m$ and $cp_m$
  **for all** $k \in n$ **do**
    Nominate node $max(w_k)$ and node $max(cp_k)$ for election
  **end for**
  After election votes are counted and nodes such as $CH$, $ACH$ and $IH$ are elected
  $P_m = \sum_{k \in n}(Vt_m(W, k)).Fb.\gamma_m$ and Cost $C_m = \frac{1}{W_m} * (W_l - W_m)\sum_{k \in n}(Vt_m(W, k))Fb.\gamma_m$
  $CH$ new reputation, $R_{CH} = R_{CH} + P_{CH} - C_{CH}$
  **for all** $k$, $k$ is not CH in cluster **do**
    new reputation $R_k = R_k + P_k$
  **end for**
  **for all** $k \in n$ **do**
    broadcast $CH_{acknowledgent} = Vt_{CH}(k) \parallel P_k \parallel R_k$
  **end for**
  Update Election Table
**end for**

The node having higher weight and cooperation is nominated as a candidate for election. There is a possibility that the information provided by the node is false regarding its weight and cooperation. The node might show underweight and overweight situation. The under declare weight will escape it from being elected as cluster head and overweight will give it some incentives to become a cluster head. To improve the trust behavior of the nodes in a cluster, VCG model is used. The purpose of the model is to disclose false information about the node's weight.

#### 2) VICKREY, CLARKE AND GROVES (VCG) APPROACH

Vickrey, Clarke, and Groves (VCG) is a useful method, which uses the tools of game theory. This model is used to show the behavior of the nodes in a network, and stimulate the nodes for truth-telling [38]. Here in this paper, a slight modification is done to the current model to deal with IoV characteristics. Previously, the energy level of the node was considered as private information and truth-telling behavior of the VCG was used to enlighten the energy level of the node [39]. Here in our proposed model, the energy level of the node and some other parameters are used as the weight of the node. Weight of the node is private information to the node. The node weight is calculated on the basis of the mobility parameters of the node in IoV. Every node is also assigned a reputation value in real number based on reward or punishment rule. The reputation of the node increases or decreases after every election process based on the cooperation of the node.

#### 3) PAYMENT AFTER ELECTION USING VCG MODEL

There are $n$ players in the game. Each node is a player in the cluster. The nodes in the game have to reveal their weight to start the election process. The election process elects some nodes as heads and declares others as participants. Both the elected heads and participants are made some payments in the form of reputation. Every node in the game wants to increase its reputation $R$. Node with higher reputation receives more services from the network. Each node maintains a reputation table called *RTable*. The *RTable* has information about the neighbor's reputation and it is updated whenever required. Algorithm 2 presents the detail of the payment procedure.

**Algorithm 2** Operational Phase & Payment for Forwarding of Packet

**Require:** Number of nodes $n$
**Ensure:** Operation of Heads & Payment Procedure for packet forwarding
**for** $m = 1 : n$ **do**
  Three Heads assign monitoring nodes MN1, MN2 and MN3
  **if** $cp_m > k$, where $k = \lceil \frac{n}{3} \rceil$ **then**
    behavior = Cooperative;
    send $t(report) =' Cooperative'$
  **else if** $cp_m \leq k$ **then**
    behavior = Selfish;
    $t(report) =' Selfish'$
  **end if**
  $CH$ compute $IF$
  $IF_m = \frac{R_m}{\sum_{m=1}^{3} R_m}$
  $CH$ Calculate the behavior of all nodes $MN_i$
  **if** $m_{cooperative} > m_{selfish}$ **then**
    grant $P_r = R_r + PF$
  **else**
    grant $P_r = R_r - PF$
  **end if**
  **if** $t_{report}(MN_i) = t_{final}$ **then**
    grant $P_{MN_i} = R_{MN_i} + P(MN)$
  **else**
    grant $P_{MN_i} = R_{MN_i} - P(MN)$
    update $R_{Table}$
  **end if**
**end for**

##### a: PAYMENT TO A CLUSTER HEAD

Payment to the nodes is made at the end of the election process. The $CH$ receives votes from the participating nodes on the basis of which payment to the $CH$ is made. The nodes voted for the $CH$ in the election also get payment, which is the cost of the elected $CH$. The cost vector, which is the node weight is represented by $W_1, W_2, \ldots, W_n$, where $n$ is all number of nodes. The difference between the payment made and received is the gain of the $CH$.

$$P_m = \sum_{k \in n}(Vt_m(W, k)).Fb.\gamma_m \tag{8}$$

where $Vt_m(W, k)$ gives certain values in the election process (value is equal to 1 if the node $k$ votes for $m$, otherwise 0 is generated). The incentive head also decides certain fixed budget $Fb$ for every node participating in the election process (this payment is fixed and known to all nodes) and $\gamma_m$ is a node payment shown below in Eq(9).

$$\gamma_m = W_m + \frac{1}{\sum_{k \in n} Vt_m(W, k)} \times (\sum_{l \in n}(W_l)). \sum_{k \in n} Vt_l(W|W_m = \infty, k) - \sum_{l \in n}(W_l)\sum_{k \in n}(Vt_l(W, K)) \tag{9}$$

*b: CLUSTER MEMBERS PAYMENT*

Based on a fixed payment $Fb$, the total cost of the nodes is distributed by the $CH$ among the nodes (nodes that have given vote). The cost function $C_m$ computed by $CH_m$ is as follows:

$$C_m = \frac{1}{W_m} * (W_l - W_m)\sum_{k \in n}(Vt_m(W, k))Fb.\gamma_m \tag{10}$$

where $W_m$ and $W_l$ shows the highest and second highest nodes weights of the participating nodes. The elected heads deducted the total cost from its payment to calculate the reputation of itself as shown below.

$$R_m = P_m - C_m \tag{11}$$

The total cost of the nodes is divided among them based on the reputation of the node. The $CH$ announces the payment to the nodes through $CH_{ack}$ message. Standard message authentication is used to sign and verify the messages. The *RTable* is updated by each node.

### B. PAYMENT FOR PACKET FORWARDING

The $CH$ and Gateway (GW) nodes are restricted to be used as relay nodes to forward packets. The relay nodes might not forward the packets if it is not generating any benefits to it. Such selfish behavior in IoV has a negative impact on the stability of the cluster. It also affects the cluster nodes disconnections and packets drop ratio. To encourage the nodes for the messages forwarding, the nodes are endowed with incentives in the form of a reputation for each message forward. The payment scheme is made effective by the monitoring system which monitors the role of the relay nodes. The notations used in the proposed scheme are listed in Table 1.

#### 1) RELAY NODES PAYMENT

The proposed approach makes a payment on each packet forward. It makes a fixed payment called (PF), which is controlled by the incentive head. The fixed payment (PF), is done on the cooperative nature of the relay nodes. So the monitoring system is proposed, which gathers evidence of all the monitoring nodes. These evidences from all the nodes are collected to calculate behavioral decision of the relay nodes.

**TABLE 1. Summary of notations and symbols.**

| Notation | Representation of the symbol |
|---|---|
| $m$ | Cluster Head $CH$ node elected in the election Process |
| $cp_m$ | Cooperation of node $m$ |
| $R_m$ | Node $m$ reputation |
| $P_m$ | Node $m$ payment |
| $Vt_m$ | Node $k$ which voted for $m$ |
| $\gamma_m$ | Per member node cost |
| $W_m$ | Weight of node $m$ |
| $IF_m$ | Importance factor of node $m$ |
| $C_m$ | The cost function of node $m$ |

*a: COMBINED TRUST OF MONITORING NODES*

In proposed model, there are three monitoring nodes in a relay. One of the monitoring nodes is auxiliary CH, another one is the predecessor and the third monitoring node is a member node selected in a round robin manner. Each relay node creates hash [40] of the packets to keep the packet genuine and preclude the forwarder from changing the packet. Therefore, when the packet reaches the next relay node it is checked with the hash value of the forwarded packet. If the hash values are matching, it means that the packet sent is steady. In the case of non-matching, the forwarder node is termed as misbehaving and will receive negative payment and declared as a selfish node. Each node maintains a buffer for the recently forwarded packets. These packets have certain expected time to be sent next. The monitoring node sends a trust report of the behavior of the node after threshold time. Node behavior can be calculated using direct trust and indirect trust. Direct trust is calculated from the interactions of the node with its neighbor nodes. The proposed scheme has three monitoring nodes, the job of the monitoring nodes are to observe the neighbors. If the monitoring node observes any unusual behavior, it calculates the trust value using the hash function. Monitoring node constantly monitors the neighbor nodes conversation with other nodes. The monitoring is responsible for watching forwarded and drop packets of every node in the network. As there is the mobility of the nodes in the network, the node may discover new nodes and replaces the old neighbors. The assessment of the node's behavior may become difficult. In such a case, the second opinion is needed to help assess the exact trust value. Thus, indirect trust with direct trust helps in improving the overall quality of decision making. Now each monitoring node calculates total trust having direct and indirect trust values. The range of each monitoring node trust value is in the range [0,1]. At the outset each node has an initial value of 0.5. Any node having trust value greater than or equal to 0.5 is termed as a cooperative node, and if the trust value is less than 0.5 it is considered selfish node.

The trust report is their individual opinion about node intention to forward packets. The trust report will be either of the set selfish, cooperative based on the behavior of the node. The CH calculates the trust value upon receiving three trust reports from the three monitoring nodes. If the joined trust value of the cooperative behavior supersedes the selfish behavior, the forwarder is declared as genuine and gets positive payments (reputation) otherwise negative payment is received to the selfish node (punishment). In order to get similar results (avoid contradictory results), joined trust on importance factor (JIF) rule is proposed to calculate the trust based on evidence from different nodes.

#### b: JOINED IMPORTANCE FACTOR FOR TRUST CALCULATION

The aim to calculate the join importance factor is monitoring nodes can declare any node as cooperative with prejudice by having a prior mutual understanding between the participating nodes. It may also unjustly label a node to be selfish to punish it. So the importance factor is necessary to distinguish between honest and dishonest monitoring nodes in the cluster. The importance factor of the monitoring node is its honesty. The honesty of the monitoring node is directly related to its reputation. This importance factor $IF$ of the monitoring node is proportional to reputation value over the total reputation value of all the monitoring nodes in the cluster. $IF_m$ shows the importance factor of monitoring node and $R_1$, $R_2$ and $R_3$ are three monitoring nodes participating in the relay.

$$IF_m = \frac{R_m}{\Sigma_{m=1}^{3} R_m} \tag{12}$$

It is assumed that if any node $m$ reports the behavior of any node $n$, the true judgment is equal to the importance factor (IF) of a node which reports the behavior of the node. So any node $m$ with importance factor $IF_m$ reports that node m is cooperative then,

$$M_m(Cooperative) = IF_m \tag{13}$$

$$M_m(Selfish) = 1 - IF_m \tag{14}$$

Similarly if any node $J$ reports $k$ as selfish then,

$$M_j(Selfish) = IF_m \tag{15}$$

$$M_j(Cooperative) = 1 - IF_j \tag{16}$$

The combined evidence will be used as a final trust to decide the honesty of the forwarder to grant payment. The selfishness and cooperativeness of the node are decided by the JIF rule. The rule is that even if two monitoring nodes claim a node to be selfish but the calculated final trust is less than the third monitoring node that claims the node to be cooperative, the node will be declared as cooperative. It means if a node is cooperative for a longer time in a cluster has its importance. Finally, the new reputation is calculated from the granted payment and current reputation of the node, and it is announced by the $CH$.

#### 2) MONITORING NODE PAYMENT

The monitoring nodes get payment for the submission of each trustworthy report. The cluster head makes the payment on some trust value. The final value determines the monitoring nodes trustworthiness. For ($PM > 0$), it means that the final trust value is matching the trust report and is declared as trustworthy monitoring node. For ($PM < 0$), the final trust value is deviated from the trust value and declared as misbehavior monitoring nodes. This model is adopted with a slight modification to deal with the characteristics of different devices in the cluster. Thus, the weight of the node is considered private information, which is one of the eligibility criteria for participating in the election. Besides, the reputation of the node is a real number assigned to each node on the basis of reward and punishment standard. The reputation of the node fluctuates on the truth-telling behavior of the participated nodes.

#### 3) REPUTATION CARRY-FORWARD

Initially, the reputation of all the nodes is set to zero as they enter the network. The reputation value of the nodes changes during the election process. The change in the reputation value is updated and announced by the $CH$ periodically during the election process. The node changes its state to $GW$ as it receives updates from another $CH$. The node shares its $RTable$ with both CHs and it continues as there is update in the $RTable$ of either cluster. Cluster heads (CH) in the network verify the genuineness of the data broadcasted by the $GW$ node. It means that $CH$ knows about all the reputation information of the nodes in two hop cluster in both directions. For example, there are three clusters $X$, $Y$, and $Z$. Suppose new node $N$ enters into cluster $Y$. According to the proposed model, cluster $Y$ knows all the reputations value of all the nodes in the $X$ and $Z$. So the node N's reputation value is known to cluster $Y$ even before it enters into $Y$. If the $CH$ is unaware of the new node reputation value, then a new node will be accepted as a new node in the network.

### C. PUNISHMENT FOR SELFISH NODES

Some of the nodes having selfish behavior are encouraged by the cluster head to take part in the election process. This makes the nodes as cooperative nodes. The cluster head can punish the node with repeated selfish behavior in three ways. When the selfish node behaves selfishly for the first time then cluster head still encourages the node for cooperation but zero incentive is given in this case. Secondly, negative payment is done after warning given by a cluster head. Lastly, a node can be expelled from the network as punishment for a specific time. But sometime a node may join the network again and behave cooperatively, so in this case, it should pay the negative incentive first.

## IV. PERPORMANCE EVALUATION

The performance of the proposed scheme IPS is evaluated using VDTNSim. VDTNSim is the extension of the

Opportunistic Environment Simulator (ONE). Due to some matching characteristics of VANET and VDTN, the two can be used in similar applications and scenarios. The delay tolerant networks are a remedy for all those scenarios where there is highly delayed and frequency of partitioning as in vehicular ad-hoc network VANET. The VDTNsim is updated constantly to add new features of the delay tolerant network [41], [42]. VDTNsim has the added capability of generating node movement, support for different nodes, support for the conventional DTN routing protocols and generating reports about message delivery and other general statistics [41]. The source code is open and is freely available [42]. One of the important characteristics of the delay tolerant network is a store-carry and forward mechanism, VDTNsim offers support for creating simulation scenarios with nodes having different characteristics.

### A. SIMULATION SETUP

Our simulation scenario consists of trams, pedestrian, and cars. The scenario has 120 numbers of nodes. The nodes are distributed as 110 pedestrians, 5 trams, and 5 cars. The simulation time is 3 hrs having 0.1s of time. The total numbers of misbehaving nodes are from 10% to 70% over the total nodes. The misbehavior of trams is not considered. Cluster-based mobility model is used in our simulation scenario. The area of one cluster is 3.5 × 2.8 km. We have used trams as an intermediate node a message ferry [43] to connect two clusters in the scenario. The pedestrians have a relative speed of 0.5 m/s to 1.5 m/s between the clusters. The trams have different speeds ranging from 4 to 6 m/s. The pause time of trams between its destinations is from 10 to 25 seconds. The moving speed of the cars is from 2.7 m/s to 13.9 m/s. Two nodes in a range can communicate with each other. The nodes can communicate in a 10 meters range. It is two-way communications at a constant rate of 2 Mbit/s. A source node randomly chooses a destination to generate a message every 10 to 15 minutes. The trams only carry a message and thus cannot generate messages. The behavior of the nodes remains static over a period of time. Time-To-Live of the generated message is 100 hrs to 120 hrs. The size of the generated messages is 100 KB to 2 MB. The buffer size of the nodes varies. The buffer size of pedestrians is 20 MB and for trams, it is 100 MB.

### B. METRICS

The simulation uses end-to-end delays, packet delivery ratio (PDR), average cost and overhead as metrics of performance in a network. IPS is compared with the following incentive based protocols: PROPHET-Selfish [44], SimBet [45] and Social selfishness Aware Routing (SSAR) [26] . SimBet protocol is used as a benchmark.

### C. RESULTS AND DISCUSSION

The payments to the nodes are done through VCG model. The nodes participating in the election process gets payment for showing cooperation in a network and can become Cluster Head, Auxiliary Cluster Head and Incentive Head through the election process. The nodes with selfish behavior and not showing the required responsibility gets negative payments as a reward. When nodes are showing selfish behavior repeatedly, then it is punished in the form of expulsion from the network.

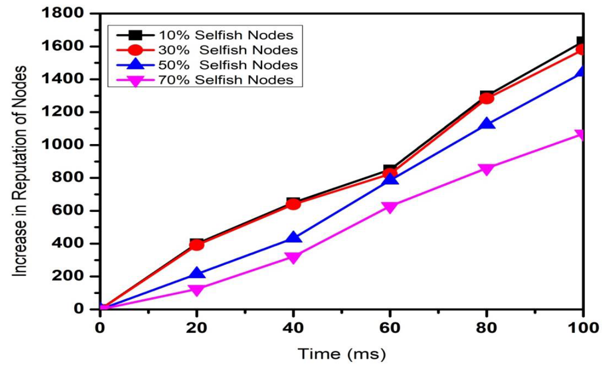


**FIGURE 2.** Reputation of nodes with selfishness.

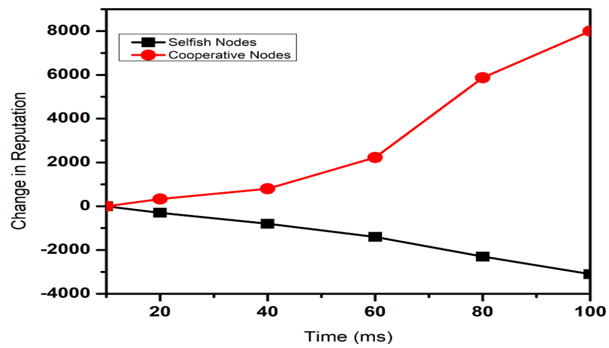


**FIGURE 3.** Variation in reputation over simulation time.

#### 1) VARIATION IN REPUTATION

The reputation of the nodes changes with the behavior of the nodes. The selfish and cooperative nature of the nodes determines the reputation of the nodes. FIGURE 2 shows fluctuation in nodes behavior in simulation during the process of election. The simulation shows selfish nodes in the network decreases the number of participated nodes in the election process. More selfish nodes in the network lower the payments by the different heads and the participated nodes. The node behavior is shown in FIGURE 3.

The simulation results show that the reputation of the nodes increases as the cooperation increases and decreases with selfish behavior. The reputation of cooperative nodes shows a higher ratio of increase in reputation than the selfish node reputation. It is due to the fact that the payment made to the nodes in the election process varies and increases in bulks are dependent on the number of nodes participating in the election process. It is also to be noted that the payment made to the relay node and monitoring nodes are fixed and depends

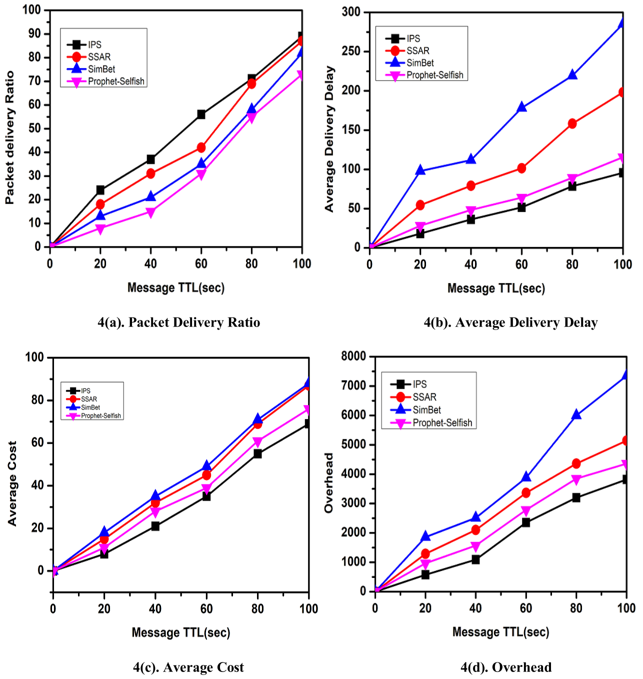


**FIGURE 4.** **Comparisons of the schemes for message TTL (second) when 50% nodes are selfish.**

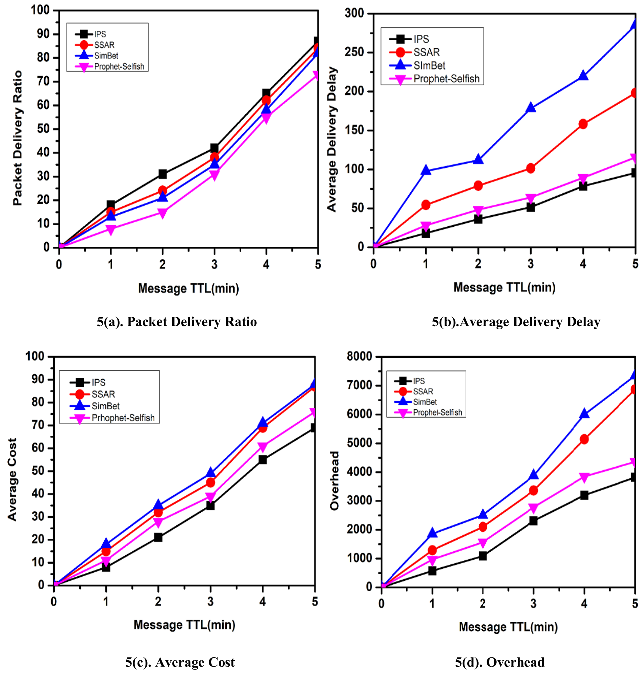


**FIGURE 5.** **Comparisons of the schemes for message TTL (minutes) when 50% nodes are selfish.**

on the behavior of node while forwarding messages. So it is clear that an increase in the reputation of nodes depends on participating in the election process and messages forwarding. The reputation decreases only in forwarding when negative payments are made.

### 2) IMPACT OF MESSAGE TTL

Packet delivery ratio, delay, cost, and overhead is used to measure the performance of the routing protocols as the TTL metric varies. In Fig. 4(a), the delivery ratio of the IPS scheme is higher. When TTL is 80 sec, the delivery ratio of IPS is 7%, 14%, and 11% higher than SSAR, Prophet-Selfish and SimBet respectively.

The core reasons are that that the proposed method omits the selfishness inside the cluster by stimulating the selfish nodes to transmit data and cooperate with the other nodes on one hand. On another hand it encourages the interactions of the nodes for better performance and high efficiency. The other three methodologies have not shown the impact of selfishness on the network in detail. The Figs. 4(b), 4(c), and 4(d) have examined the performance metrics of the routing protocols (average delivery delay, cost, and overhead) by different methods. The performance metrics (Average delivery delay, Average cost, and Overhead) continuously grows when there is an increase in message TTL. The reason is that the network drops the messages for little benefits. Comparatively, the IPS scheme has the minimum delay, overhead, and cost. When the TTL is 80 sec, the delay of IPS is 3%, 26%, and 47% lower than Prophet-Selfish, SSAR and SimBet respectively.

The cost of IPS is approximately 6%, 14%, and 16% lower than Prophet-Selfish, SSAR, and SimBet respectively. Similarly, the overhead of IPS is approximately 9%, 15%, and 35% lower than Prophet-Selfish, SSAR, and SimBet respectively. It is seen that average delay and cost is still added as the average ratio increases with an increase in TTL message. It is seen in Fig. 5(a), Packet delivery ratio of IPS grows steadily as the TTL enhances. When the TTL is 4 minutes, IPS outperforms SSAR, SimBet, and Prophet-Selfish by around 3%, 7%, and 10% respectively. The core reason is that IPS encourages selfish nodes to stimulate and behave cooperatively in the network. This is in contrast to the SSAR, SimBet, and Prophet-Selfish, where nodes take Similarly, IPS also outperforms all these schemes in term of cost and overhead. When the TTL is 4 minutes, the cost of IPS is 6%, 14%, and 16% lower than Prophet-Selfish, SSAR, and SimBet respectively as shown in Fig. 5(c). Similarly, the overhead of IPS is 9%, 25%, and 35% lower than Prophet Selfish, SSAR, and SimBet respectively as shown in Fig. 5(d). This is due to the reason that monitoring nodes in IPS properly monitor the behavior of all nodes in the network.

### 3) IMPACT OF VARYING SELFISH NODES

These algorithms are compared for obtained network properties as shown in FIGURE 6, in case 10%, 30%, 50%, and 70% of nodes are selfish in nature. The performances gained by IPS outperform SSAR, SimBet and Prophet-Selfish mechanism in term of delivery ratio as shown in Fig. 6(a).

In the other methods like SSAR, prophet- selfish, and SimBet the nodes decide the data forwarding operation by their interaction history and the nodes selfishness cannot be regulated dynamically. For 50% selfish nodes, the delivery

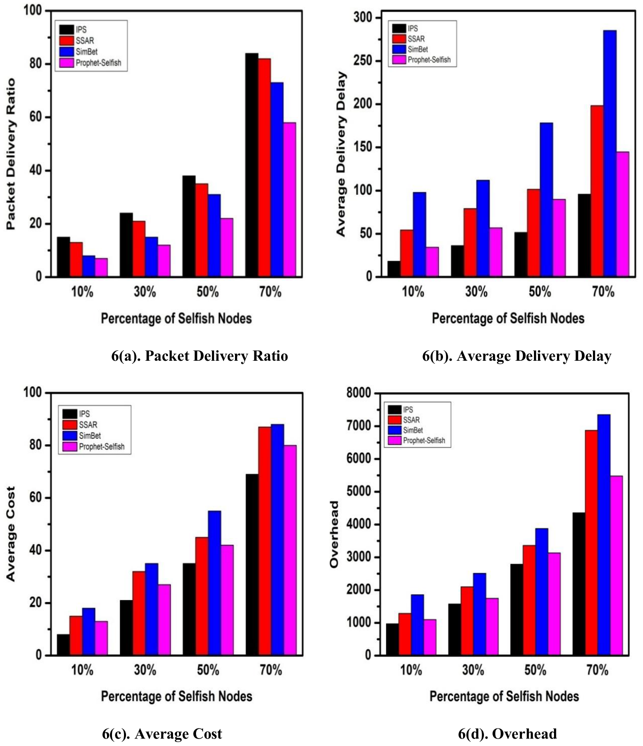


**FIGURE 6.** Comparisons of the Schemes for different percentage of selfish nodes.

ratios of IPS, Prophet-Selfish, SSAR, and SimBet are respectively 38, 22, 35, and 31. Thus, the packet delivery ratio of IPS is approximately 3%, 7%, and 16% higher than SSAR, SimBet, and Prophet Selfish respectively because in IPS encourage the selfish nodes to transmit data in cooperative way inside their own cluster. Similarly, the IPS scheme outperforms SSAR, SimBet and Prophet-Selfish in term of average delay, cost and overhead as shown in Figs. 6(b), 6(c), and 6(d). For 50% selfish nodes, the average delay of the IPS are 12%, 16%, and 42% lower than Prophet-Selfish, SSAR and SimBet schemes respectively as shown in fig. 6(b). Similarly, the average cost of IPS is 11%, 21%, and 31% lower than Prophet-Selfish, SSAR, and SimBet schemes respectively. In addition, for 50% selfish nodes in the network, the overhead of IPS are 14%, 31%, and 37% lower than Prophet-Selfish, SSAR and SimBet schemes respectively. It is due to the fact that in the other methods the nodes deny forwarding messages to its neighbor nodes if it has no strong social relationship with its neighbors. In SimBet and SAAR methods it is assumed that the nodes are cooperative residing in the same cluster. So the percentage of selfishness is small in this protocol. While in our method of IPS the nodes can adjust their selfishness accordingly if it has enough credit for data forwarding. This increases network performance by dynamically adjusting the node selfishness. Fig. 6 concludes that IPS has a greater capacity to absorb the selfishness of the nodes and stimulate the nodes to cooperate in the network for better performance.

## V. CONCLUSION AND FUTURE WORK

In this paper, Incentive and Punishment scheme is proposed for IoV to encourage the selfish nodes in the cluster to forward messages. This scheme detects selfish nodes and monitors their behavior constantly. The incentive is given in the form of reputation that makes the node cooperative within the network. Nodes are also punished for showing repeatedly selfish behavior. The monitoring nodes monitor the performance of their neighbor nodes after the election process. Three protocols SSAR, SimBet and Prophet-Selfish are simulated extensively to evaluate the performance of packet delivery ratio, average delay, average cost and overhead. The results shows that IPS can potentially accommodate a large set of selfish nodes by stimulating more selfish nodes to cooperate in a cluster to improve network performance. In future work, the bandwidth utilization should be based on the reputation of nodes participating in the network during service delivery. Also the nodes have small contacts (short time contacts) with one another. Thus, such contacts need further improvement so that communication becomes more meaningful.

## REFERENCES

[1] L. Maglaras, A. Al-Bayatti, Y. He, I. Wagner, and H. Janicke, "Social Internet of vehicles for smart cities," *J. Sens. Actuator Netw.*, vol. 5, no. 1, p. 3, 2016.
[2] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2627–2637, Aug. 2018.
[3] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in Internet of vehicles: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015.
[4] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.
[5] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, Oct. 2018.
[6] T. S. J. Darwish and K. A. Bakar, "Fog based intelligent transportation big data analytics in the Internet of vehicles environment: Motivations, architecture, challenges, and critical issues," *IEEE Access*, vol. 6, pp. 15679–15701, 2018.
[7] Y. Yang, Y. Wu, N. Chen, K. Wang, S. Chen, and S. Yao, "LOCASS: Local optimal caching algorithm with social selfishness for mixed cooperative and selfish devices," *IEEE Access*, vol. 6, pp. 30060–30072, 2018.
[8] N. Liu, "Internet of vehicles: Your next connection," *Huawei WinWin*, vol. 11, pp. 23–28, Dec. 2011.
[9] R. Buyya and A. V. Dastjerdi, *Internet of Things: Principles and Paradigms*. Amsterdam, The Netherlands: Elsevier, 2016.
[10] B. B. Dubey, N. Chauhan, N. Chand, and L. K. Awasthi, "Incentive based scheme for improving data availability in vehicular ad-hoc networks," *Wireless Netw.*, vol. 23, no. 6, pp. 1669–1687, 2017.
[11] S. Xu, M. Li, Y. Chen, L. Shu, and X. Gu, "A cooperation scheme based on reputation for opportunistic networks," in *Proc. Int. Conf. Comput., Manage. Telecommun. (ComManTel)*, Jan. 2013, pp. 289–294.
[12] S.-C. Lo, Y.-J. Lin, and J.-S. Gao, "A multi-head clustering algorithm in vehicular ad hoc networks," *Int. J. Comput. Theory Eng.*, vol. 5, no. 2, p. 242, 2013.
[13] J. A. F. F. Dias, J. J. P. C. Rodrigues, C. X. Mavromoustakis, and F. Xia, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7929–7937, Dec. 2015.
[14] Y. Li, G. Su, and Z. Wang, "Evaluating the effects of node cooperation on DTN routing," *AEU-Int. J. Electron. Commun.*, vol. 66, no. 1, pp. 62–67, 2012.

[15] Y. Li, G. Su, D. O. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 5, pp. 2224–2238, Jun. 2011.
[16] J. A. F. F. Dias, J. J. P. C. Rodrigues, L. Shu, and S. Ullah, "Performance evaluation of a cooperative reputation system for vehicular delay-tolerant networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 88, 2014.
[17] 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)*, Aug. 2018, pp. 34–39.
[18] H. Wei, Y. Zhang, D. Guo, and X. Wei, "CARISON: A community and reputation based incentive scheme for opportunistic networks," in *Proc. 5th Int. Conf. Instrum. Meas., Comput., Commun. Control (IMCCC)*, Sep. 2015, pp. 1398–1403.
[19] T. Zhang and F. Wu, "Stimulating traffic information transfer in non-cooperative vehicular ad hoc networks," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2014, pp. 225–230.
[20] Z. Ning, L. Liu, F. Xia, B. Jedari, I. Lee, and W. Zhang, "CAIS: A copy adjustable incentive scheme in community-based socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3406–3419, Apr. 2017.
[21] B. Jedari, L. Liu, T. Qiu, A. Rahim, and F. Xia, "A game-theoretic incentive scheme for social-aware routing in selfish mobile social networks," *Future Gener. Comput. Syst.*, vol. 70, pp. 178–190, May 2017.
[22] H. Zhou, J. Wu, H. Zhao, S. Tang, C. Chen, and J. Chen, "Incentive-driven and freshness-aware content dissemination in selfish opportunistic mobile networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 9, pp. 2493–2505, Sep. 2015.
[23] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda, "Barter trade improves message delivery in opportunistic networks," *Ad Hoc Netw.*, vol. 8, no. 1, pp. 1–14, 2010.
[24] L. Liu, Q. Yang, X. Kong, H. B. Liaqat, A. M. Ahmed, N. Deonauth, and F. Xia, "Com-BIS: A community-based barter incentive scheme in socially aware networking," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, 2015, Art. no. 671012.
[25] M. M. Umar, S. Khan, R. Ahmad, and D. Singh, "Game theoretic reward based adaptive data communication in wireless sensor networks," *IEEE Access*, vol. 6, pp. 28073–28084, 2018.
[26] Q. Li, W. Gao, S. Zhu, and G. Cao, "A routing protocol for socially selfish delay tolerant networks," *Ad Hoc Netw.*, vol. 10, no. 8, pp. 1619–1632, 2012.
[27] J. Liu, L. Bic, H. Gong, and S. Zhan, "Data collection for mobile crowd-sensing in the presence of selfishness," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 82, 2016.
[28] A. Jesudoss, S. K. Raja, and A. Sulaiman, "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme," *Ad Hoc Netw.*, vol. 24, pp. 250–263, Jan. 2015.
[29] W. Fawaz, "Effect of non-cooperative vehicles on path connectivity in vehicular networks: A theoretical analysis and UAV-based remedy," *Veh. Commun.*, vol. 11, pp. 12–19, Jan. 2018.
[30] X. Li and J. Wang, "A generous cooperative routing protocol for vehicle-to-vehicle networks," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 11, pp. 5322–5342, 2016.
[31] A. Socievole, A. Caputo, F. De Rango, and P. Fazio, "Routing in mobile opportunistic social networks with selfish nodes," *Wireless Commun. Mobile Comput.*, vol. 2019, Feb. 2019, Art. no. 6359806.
[32] F. De Rango, A. Socievole, and S. Marano, "Exploiting online and offline activity-based metrics for opportunistic forwarding," *Wireless Netw.*, vol. 21, no. 4, pp. 1163–1179, 2015.
[33] A. Socievole, E. Yoneki, F. De Rango, and J. Crowcroft, "ML-SOR: Message routing using multi-layer social networks in opportunistic communications," *Comput. Netw.*, vol. 81, pp. 201–219, Apr. 2015.
[34] A. Socievole, F. De Rango, A. Caputo, and S. Marano, "Simulating node selfishness in opportunistic networks," in *Proc. Int. Symp. Perform. Eval. Comput. Telecommun. Syst. (SPECTS)*, Jul. 2016, pp. 1–6.
[35] P. R. Vamsi and K. Kant, "Trust aware cooperative routing method for WANETs," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 6189–6201, 2016.
[36] U. Venkanna, J. K. Agarwal, and R. L. Velusamy, "A cooperative routing for MANET based on distributed trust and energy management," *Wireless Pers. Commun.*, vol. 81, no. 3, pp. 961–979, 2015.
[37] M. Chatterjee, S. K. Das, and D. Turgut, "An on-demand weighted clustering algorithm (WCA) for ad hoc networks," in *Proc. IEEE. Global Telecommun. Conf. (Globecom)*, vol. 3, Nov. 2000, pp. 1697–1701.
[38] A. Mas-Colell, M. D. Whinston, and J. R. Green, *Microeconomic Theory*, vol. 1. New York, NY, USA: Oxford Univ. Press, 1995.
[39] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "Mechanism design-based secure leader election model for intrusion detection in MANET," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 1, pp. 89–103, Jan. 2011.
[40] A. Sulaiman, S. K. Raja, and S. H. Park, "Improving scalability in vehicular communication using one-way hash chain method," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2526–2540, 2013.
[41] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proc. 2nd Int. Conf. Simulation Tools Techn. (Simutools)*, 2009, pp. 55:1–55:10. doi: 10.4108/ICST.SIMUTOOLS2009.5674.
[42] V. N. Soares, F. Farahmand, and J. J. Rodrigues, "VDTNsim: A simulation tool for vehicular delay-tolerant networks," in *Proc. 15th IEEE Int. Workshop Comput. Aided Modeling, Anal. Design Commun. Links Netw. (CAMAD)*, Dec. 2010, pp. 101–105.
[43] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 607–640, 2nd Quart., 2012.
[44] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," in *Proc. ACM Int. Symp. Mobilde Ad Hoc Netw. Comput. (MobiHoc)*, 2003, pp. 1–2.
[45] E. M. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant MANETs," in *Proc. 8th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2007, pp. 32–40.

**GHANI-UR-REHMAN** received the bachelor's degree in computer science from the Kohat University of Science and Technology, Kohat, and the M.S. degree in computer science from the Department of Computer Science and Software Engineering, International Islamic University Islamabad, where he is currently pursuing the Ph.D. degree with the Department of Computer Science and Software Engineering. He is currently a Lecturer with the Department of Computer Science, Khushal Khan Khattak University, Karak. His research interests include wireless communication systems, future networks, the Internet of Things, and particularly focusing on topics related to mobility and QoS.

**ANWAR GHANI** received the B.S. degree in computer science from the University of Malakand, Pakistan, in 2007, and the M.S. degree in computer science and the Ph.D. degree in computer science from the Department of Computer Science and Software Engineering, International Islamic University Islamabad, in 2011 and 2016, respectively. He is a Faculty Member of the Department of Computer Science and Software Engineering, International Islamic University Islamabad. He was a Software Engineer with Bioman Technologies, from 2007 to 2011. He was selected as an exchange student through the EURECA Program with VU University Amsterdam, The Netherlands, in 2009, and the EXPERT Program with Masaryk University, Czech Republic, in 2011, supported by the EUROPEAN Commission. His broad research interests include wireless sensor networks, next generation networks, information security, and energy efficient collaborative communication.

**MUHAMMAD ZUBAIR** received the bachelor's, master's, and M.S. degrees in computer science from the University of Peshawar, Pakistan, and the Ph.D. degree in communication and information system from the Dalian University of Technology, China. He is currently an Assistant Professor with the Department of Computer Science, Khushal Commercialization (ORIC), Khushal Khan Khattak University, in August 2015, where he was the Founding Director of ORIC, until February 2017. He has received the title of Entrepreneurial Scientist by the South Asian Triple Helix Association, in 2018, and included his name in the list of top twenty entrepreneurial scientist, published in the book with the title Entrepreneurial Scientist Serving-Science and Society. He was awarded the SATHA Innovation Award from the Third Invention to Innovation Summit 2017, UET Peshawar. He was a master trainer by Intel, Pakistan. He is a Reviewer of several well reputed journals and conferences. His research interests include wireless communication systems, future networks, the Internet of Things, and particularly focusing on topics related to mobility, QoS, and security. He also got several technology awards for his innovative projects.

**SYED HUSNAIN A. NAQVI** received the Ph.D. degree from The University of Auckland, New Zealand. He has more than 16 years teaching, and research and development experience in New Zealand and Pakistan. He was with several multi-national software companies as a software developer, a consultant, and the technical manager. He is an author of more than 70 peer-reviewed journals, international conference papers, and book chapters. Over the last 16 years, he has supervised over 80 students pursuing the M.S. and Ph.D. degrees, summer research, or final year projects. He has several Academic/Industrial Certificates that include MCPS, MCITP (Database Developer 2008 and Database Administrator 2008), MCTS [(Microsoft Office Visio 2007 and Application Development, SQL Server 2008, Implementation and Maintenance, SQL Server 2008, Database Development, SQL Server 2008, Business Intelligence Development and Maintenance, SharePoint 2010, Application Development,.NET Framework 4, Windows Applications,.NET Framework 4, and Service Communication Applications), and MCSA( SQL Server 2008)]. His broad research interests include sensor networks, collaborative communications, and lightweight cryptography.

**DHANANJAY SINGH** (SM'14) received the B.Tech. degree in computer science and engineering from Veer Bahadur Singh Purvanchal University, Jaunpur, India, in 2003, the M.Tech. degree in wireless communication and computing from the Indian Institute of Information Technology, Allahabad, India, in 2006, and the Ph.D. degree in ubiquitous IT from Dongseo University, Busan, South Korea, in 2010. He has been the Director of the ReSENSE Laboratory, Hankuk University of Foreign Studies, Yongin, South Korea, since 2012, where he is also an Assistant Professor with the Department of Electronics Engineering and the Chair of the Division of Global IT. He was a Postdoctoral Researcher and a Senior Member Engineering Staff of future internet architecture with the National Institute of Mathematical Sciences and the Electronics and Telecommunication Research Institute, Daejeon, South Korea, from 2010 to 2012. He has published 100+ refereed scientific papers, served 100+ TPC membership, and delivered 50+ invited talks in major IEEE conferences/workshops. His research interests include the design, analysis, and implementation of algorithms/protocols for large-scale data set to solve real-world problems specifications future internet architecture for the smart city and IoT services. He is a Senior Member of the ACM Society. He has won three times best paper awards from IEEE conferences and two times the fellowship award from APAN meeting at Singapore and Manila.

**SHAD MUHAMMAD** received the master's degree in computer science from the Department of Computer Science, University of Peshawar, and the M.S. degree in computer science from London Metropolitan University, U.K. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Kohat University of Science and Technology, Kohat. He is currently a Lecturer with the Department of Computer Science, Khushal Khan Khattak University, Karak. His research interest include wireless communication systems, the future networks, the Internet of Things, and particularly focusing on topics related to cloud computing and mobile computing.