

Article

Performance Evaluation and Comparison of Cooperative Frameworks for IoT-Based VDTN

Ghani Ur Rehman ¹, Muhammad Zubair ^{1,*} , Wael Hosny Fouad Aly ^{2,*} , Haleem Farman ³, Zafar Mahmood ⁴, Julian Hoxha ²  and Naveed Anwer Butt ⁴ 

¹ Department of Computer Science and Bioinformatics, Khushal Khan Khattak University, Karak 27000, Pakistan

² College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait

³ Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan

⁴ Department of Computer Science, University of Gujrat, Gujrat 50700, Pakistan

* Correspondence: dr.muhammadzubair@kkuk.edu.pk (M.Z.); wael.alay@aum.edu.kw (W.H.F.A.)

Abstract: The term “Internet of Things” (IoT) refers to an architecture in which digital objects have identification, sensing, connectivity, and processing capabilities that allow them to connect with other devices as well as perform tasks on the internet. There are many applications of IoT, among which Vehicle Delay-Tolerant Networks (VDTNs) are one of the best known. This new generation of vehicular networks can be applied in a variety of circumstances. For example, it can be employed to make data connections possible in densely crowded cities and as well as in remote and sparsely populated places with weak connectivity. These environments are characterized by frequent network partitioning, inconsistent connectivity, considerable propagation delays, high error rates, and short contact duration. Most of these behaviours are due to node selfishness. This task is crucial because selfish behaviour by nodes may make other nodes hesitant to cooperate. Selfish nodes have significant negative impacts on the effectiveness and efficiency of the network as a whole. To solve these issues, cooperative strategies that motivate nodes to share their resources must be considered. Important contributions to cooperation for vehicular networks are presented in this article, which investigates the effects of six different cooperative techniques on network performance and makes corresponding suggestions for their use in IoT-based VDTNs. Across all simulations, our results show that the studied strategies are all able to increase overall network performance by improving throughput and packet delivery probability, which in turn reduces average packet delivery time, energy consumption, overhead ratio, and the number of packets dropped.

Keywords: Internet of Things (IoT); cooperation; selfishness; VDTNs; incentive; store; forward and carry approach



Citation: Rehman, G.U.; Zubair, M.; Aly, W.H.F.; Farman, H.; Mehmood, Z.; Hoxha, J.; Butt, N.A. Performance Evaluation and Comparison of Cooperative Frameworks for IoT-Based VDTN. *Sustainability* **2023**, *15*, 5454. <https://doi.org/10.3390/su15065454>

Academic Editor: Lei Miao

Received: 20 January 2023

Revised: 9 March 2023

Accepted: 10 March 2023

Published: 20 March 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In order to connect the real and virtual worlds with advanced technologies, the Internet of Things (IoT), a global smart device infrastructure, is currently being developed [1–3]. Objects attempt to communicate data across network devices on the IoT, which is a smart network. IoT has astounding applications in every aspect of human existence, including smart communities, smart environments, intelligent water control, safety and emergency systems, smart transportation, smart farming, industrial control, and healthcare [4–6]. Its goals are to simplify work and improve quality of life. The IoT is well known for its capacity to connect various objects to the digital world [7]. The advancement of wireless communications has made it possible for the Internet of Things to send and receive data packets [8,9].

IoT devices have a variety of applications. They are widely used in Vehicular Delay-Tolerant Networks [10]. VDTNs have been recommended as a way to deal with a number of challenges associated with vehicle networks. The majority of these problems today have

direct consequences on how vehicles behave, e.g., speed and mobility. For instance, the network architecture is continually changing due to the high level of mobility, which causes irregular connectivity and consequently leads to high loss percentages [11,12].

Various vehicular communication architectures are used in vehicular networks environments, such as Vehicular Ad hoc Networks (VANETs) [13] and Delay Tolerant Networks (DTNs) [14], and have made substantial contributions that are included in vehicular delay-tolerant networks. The network architecture from VANETs, for instance, has been widely taken into consideration. Vehicles can connect directly in VDTNs, creating vehicle-to-vehicle communication, or they can interact with roadside infrastructures, creating a vehicle-to-infrastructure connection [15]. Another option is a hybrid design that takes the best features of both techniques.

The popular store-carry-and-forward model suggested for DTNs is used by VDTNs [16–18]. Using this mechanism, vehicles can receive a message, store it, and then send it to any new vehicle that enters their communication range. Data are transmitted using a particular routing protocol when a communication possibility becomes available. This process continues until the information arrives at its intended destination. VDTNs take into account three network types: mobile, relay, and terminal nodes. The bundle aggregation and dis-aggregation activities are carried out by terminal nodes (possibly stationary or mobile), which are positioned at the network's edge. Relay nodes are stationary storage-capable devices positioned at junctions to increase the number of interactions among nodes in the network. By increasing the total number of delivered bundles and reducing the typical transmission delay, an increase in communication possibilities boosts network performance in general [19,20]. Bundles are kept in such nodes until a viable communication possibility is available to transfer them closer to their destination. Furthermore, many VDTN node types connect with mobile nodes (vehicles) that move across roads. The adoption of smart nodes as terminal nodes is possible as well [21].

Considerable research has been carried out on enhancing the functionality of VDTN networks; however, there are several remaining problems that need to be addressed. Multi-hop communications are made available by wireless technology's limited bandwidth, and the lifetime of all these connections relies on each node's cooperation [22–24]. One of the main problems is that certain nodes inside VDTN networks do not cooperate when transferring data in multi-hop communications because of the connectivity between the devices and the internet [25]. Selfish nodes are those that fit this description in the VDTN networks. Selfish nodes do not engage in resource-saving when forwarding data packets to nearby nodes, and use the network services only to further their particular interests. Malicious nodes, on the other hand, are nodes that have a history of causing harm to the network and abusing its infrastructure [26]. As the number of such nodes grows, the bandwidth and network lifetime drop, while the average end-to-end delay, energy consumption, and network traffic all grow. This results in conflict with the requirements of good network performance [27,28]. For this reason, it is essential to investigate the most effective methods of encouraging nodes to cooperate and develop the best possible cooperative systems in order to ensure superior service and boost network performance without damaging or degrading nodes' data [29,30]. A node's ability to support advanced schedulers is vital as well.

It has to be taken into account that two different types of cooperative nodes with different behaviors can be identified when deploying either of the aforementioned cooperation methodologies. First, a node might exhibit selfish behavior, which means that nodes of this type are unwilling to offer their resources. Cooperative nodes help others by sharing their resources, in contrast to selfish nodes, though selfish nodes may influence the performance of cooperative nodes; for instance, by using a fixed or random amount of their resources, nodes can be encouraged to cooperate. To choose the amount of resource sharing, other methods take into account node performance. The following are the main contribution of this article:

- A review of the state-of-the-art that takes into consideration the most significant contributions to IoT-Based VDTN cooperation.
- Recommendations for six IoT-based VDTN cooperation methods.
- A study of the impact of node misbehavior on IoT-Based VDTN schemes using a large set of simulations.
- An evaluation and comparison of the performance of IoT-based VDTN cooperation methods in terms of different parameters, including packet delivery probability, packet delivery delay, throughput, overhead ratio, throughput, number of packets dropped, and energy consumption.

The rest of this article is organized as follows: Section 2 contains the literature review; different cooperative techniques are covered in Section 3; in Section 4, we discuss the simulation setting and compare the six cooperative frameworks for different parameters; finally, the article is concluded and future works are discussed in Section 5.

2. Related Works

IoT-based vehicular connectivity can be employed in a variety of scenarios that take into account different locations and objectives [31]. For instance, it can be applied in rural areas to facilitate interaction between sparsely populated areas. When contacts are lost due to a major incident, emergency vehicles may employ this type of connectivity. Regardless of the situation in which vehicular networks are implemented, it is essential to remember that a good routing protocol alone cannot guarantee optimal network performance. This is essential because nodes in these networks can behave selfishly or cooperatively. Selfish nodes could be the property of specific users who are reluctant to share their resources in order to convey information to all other users. Sharing resources without obtaining something in return is not acceptable to these nodes. Cooperative nodes are nodes that move along roadways, increasing the chances of their meeting and connect with many other nodes. These nodes are typically picked as message forwarders. However, if a node is chosen as a message forwarder, then it might be forced to diverge from the system in order to preserve its information and resources. Offering incentives to these two types of nodes as a reward for their cooperative activity is crucial to developing a system that combines the advantages of these two types of nodes.

Various approaches to cooperation are addressed in this article. For instance, we consider four different types of incentives for cooperative activity in IoT-based VDTNs [32,33]. The first determines whether a node behaves well and is appropriate for communication using its reputation. A node is labeled as a non-cooperative node when it has a poor reputation. As a result, this node's communication requests are ignored by the other nodes. Typically, reputation-based strategies involve this kind of incentive [34–36]. The second incentive technique is called the credit-based technique, in which nodes receive credits as a reward for their cooperative behavior [37–39]. The third type of incentive strategy is called the hybrid strategy, which combines both reputation and credit-based schemes [40,41]. The fourth incentive scheme is known as the game-theoretic scheme, in which socially selfish nodes are encouraged to take part in all routing processes in the network [42,43]. In the context of IoT-based vehicle networks, these four incentive kinds are all taken into account.

Regarding VANETs, many strategies and solutions have been put forward to enhance the performance of the network by encouraging node cooperation. For example, in [44] the authors proposed Distributed Approach (DASH), a new reputation mechanism to tackle the issue of selfishness in the network. They decided to simply avoid communication with selfish nodes until they begin to fully cooperate instead of permanently removing them from the network. In this way, the selfish nodes have a chance to improve their behavior, participate in packet forwarding, and ultimately boost the performance of the network. Sharma et al. [45] proposed a new deep autoencoder-based non-negative matrix factorization (DANMF) to deal with the selfishness problem. Efficient cluster formation results from the architecture of social links mapped onto low-dimensional space. DANMF uses the characteristics of the information to automatically generate a suitable nonlinear

mapping function. Additionally, the basic architecture of the deep auto-encoder is nonlinear and highly flexible. The weighted cumulative social tie, which is ultimately employed in conjunction with the residual energy to identify the network's selfish node, is designed using the participation matrices derived from the DANMF.

To encourage selfish nodes to collaborate in data forwarding, the authors of [46] proposed a Copy Adjustable Incentive Scheme (CAIS). In CAIS, they discussed a network where the nodes are separated into specific communities based on their social connections. The nodes are then rewarded when they relay data to other nodes inside or outside of their community, respectively, by applying different kinds of credits, namely, social credit and non-social credit. According to this methodology, a node's ability to reproduce messages to other nodes is changed following its level of collaboration and gained rewards. A single-copy data replication policy is used to handle the credit allocation among all nodes in response to its resource availability, which further boosts CAIS performance. The work of [47] describes a method to identify a node's selfishness based on its message forwarding and dropping behaviour and describes an innovative credit-based mechanism to encourage nodes to participate in message forwarding. The proposed technique was applied to the well-known Bubble Rap social-based routing algorithm. Hasani et al. [48] presented a new social network-based method for fuzzy-based selfish node identification in ad hoc networks. To avoid isolating the possibly selfish nodes from the system while maintaining as many active nodes within the network as possible, the presented social-based approach used three factors to measure the status of the node: hop count ($H.C.$), residual energy ($Re - En.$), and cooperation history ($Co - h.$). These variables were used to assist the nodes' status through a fuzzy interface process.

The authors of [49] presented the Game-theoretic Incentive Scheme for Social-aware (GISSO) routing to promote Socially Selfish (SS) nodes in packet relaying and guarantee that routing efficiency is optimized when SS nodes adhere to the system. They first assess the social utility of each message to an intermediary node based on the strength of the social connections and communication features. Then, to increase the social utility of SS nodes, they incorporate a game of bartering with alternate offers. Guo et al. [50] proposed a technique that addressed the issue of cooperative nodes lacking extensive understanding of one another. The authors created a game algorithm to increase the utility of nodes. Using the game algorithm, selfish nodes can be encouraged to cooperate effectively within a network. For interest-based social-aware forwarding in the DTNs, Haq et al. [51] proposed an incentive-aware pricing game. To improve content delivery in DTNs, they constructed the pricing game between nodes as a Rubinstein Bargain model based on the following three factors: (1) the degree of remaining battery performance, (2) the strength of the social connections, and (3) the value of the messages, where the communication nodes determine the price and the degree of cooperation. Additionally, the proposed technique permits nodes to exchange information in a peer-to-peer manner, which improves the content delivery of larger messages in these kinds of networks.

Sharma et al. [52] presented a credit-based mechanism dependent on the cumulative trust value (CTV) for DTN. Their proposed method is based on the computation of each node's trust value on the number of messages transmitted by sensor nodes through an actor. Credits are allocated to nodes in a distributed fashion using this trust value, with no favoritism to certain nodes. Credits are distributed to boundary nodes that deserved credit but did not receive it from the actor node using the backtracking methodology. Jethawa et al. [53] proposed a framework for calculating incentives taking into account variables such as message quality, level of interest, energy requirement, etc. They developed a distributed reputation model (DRM) linked with the proposed incentive mechanism to keep the nodes from becoming harmful by adding inappropriate message labels to obtain more incentives. DRM takes information from intermediary users, such as assessments of the message's quality and the applicability of its annotations. Thus, the proposed approach assures that congestion caused by self-centered nodes in the system is avoided. The authors of [54] expanded previously suggested reputation systems to use a hybrid system, with

the major objective being to persuade self-centered nodes to share their resources with others rather than instantly kicking them out of the network. Along with the concept of this hybrid system, two incentive mechanisms were established.

In this section, we have discussed the most significant techniques that have been originally presented to address cooperation difficulties in vehicular networks. These techniques can be used as a foundation to develop innovative IoT-based VDTN cooperation schemes.

3. Cooperation Strategies for IoT-Based VDTNs

IoT-Based VDTNs rely on network node collaboration to behave well in a variety of circumstances. Cooperation between nodes can occur throughout a communication possibility at two distinct levels, taking into account both the control and data planes. At the level of the control plane, nodes work together by communicating relevant information (such as communication time and duration, node location, speed, and storage capacity), which makes it possible to estimate contacts' availability for exchanging data relatively correctly. To optimize the use of data connection resources, nodes might interact at the data plane level by distributing their resources (such as link bandwidth and storage capacity) with one another. Additionally, sending packets from others that are stored by nodes is another possible approach to collaboration at the data plane. Figure 1 presents the IoT-Based VDTN cooperative communication system.

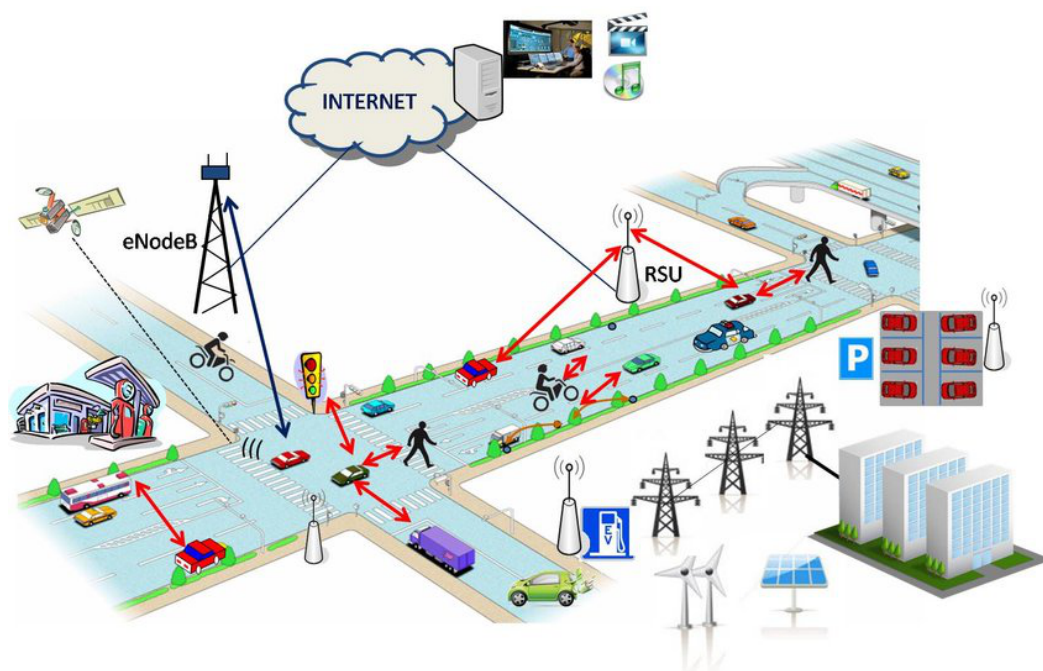


Figure 1. Internet of Things Based VDTN cooperative communication system [55].

Six important strategies for cooperation in IoT-Based VDTNs are presented in this article. The following subsections introduce and describe these six strategies and underline their key features.

3.1. Socially Omitting Selfishness in IoT for Smart and Connected Communities

This scheme, called Socially Omitting Selfishness (SOS), mostly depends on node participation in the network [56]. Nodes in the community engage in a variety of performance-related tasks, such as message forwarding, node supervision, and node tracking. The primary responsibilities of the participating nodes in the election process are thought to be these tasks. The community's nodes are encouraged to take part and work together as a unit. Monitoring the actions of the neighboring nodes is one of the key characteristics of the community-based node. A node can completely control the sending and receiving of messages according to this characteristic. Therefore, a reputation-based incentive system

is provided to encourage and motivate the nodes to perform their responsibilities in the network according to the specified scheme. Nodes with malicious or self-centered attitudes are encouraged to participate in the voting process and behave cooperatively.

When selfish nodes continually participate in misbehavior, they are punished by being removed from the community. The community is informed of this punishment. The nodes initiate involvement in the election process, which establishes the election process. The proposed system is divided into two phases: the election scheme and the payment mechanism. Elections are periodically used to control the community. During the voting process, different heads are elected based on their greater weight, level of collaboration, and number of votes. The weight and cooperation can be calculated by using Equations (1) and (2).

$$W_x = E_x \cdot wt_1 + B_x \cdot wt_2 + T_{ID_m}^x \cdot wt_3 + ND_x \cdot wt_4 + RD_x \cdot wt_5 \quad (1)$$

where E_x is the energy, B_x is the buffer, $T_{ID_m}^x$ denotes bundle delivery, ND_x is the node degree, and RD_x is the relative distance.

$$cp_x = \sum_{n \in N} Rc_n, cp_x > k \quad (2)$$

where cp_x is the cooperation of node x and Rc_n denotes the number of contacts of node x .

Selfishness is avoided by encouraging nodes to work together, which enhances the community's ability with respect to sustainability, preservation, regeneration, and attainability. By keeping a close watch on nodes using a trust value, it is possible to determine whether they are selfish or cooperative. The trust value's range is $[0, 1]$. Nodes are categorized as cooperative or selfish depending on their trust value. When the trust value is greater or equal to 0.5, the node is cooperative; otherwise, the node is considered selfish.

3.2. Honesty-Based Democratic Scheme for Community Cooperation

The proposed technique is called Honesty-Based Democratic Scheme (HBDS) [10]. The main objective is to look into node participation in the VDTN network. The network's nodes are responsible for forwarding messages and keeping a close watch on one another. The primary duties of the nodes in the democratic process are these two tasks. Nodes are motivated to join the network and cooperate to improve network performance. The node in a community-based network keeps track of how other nodes transmit and receive messages. As a result, the node has control over how messages are forwarded in a network. The presented mechanism proposes rewards to the nodes in the form of reputation to encourage stimulation and enhance network performance. The proposed mechanism demonstrates the nodes' participation in the network and their support for network performance. A node's contribution consists of message forwarding and neighbor node monitoring for message forwarding. In HBDS, nodes are nominated by a democratic process based on the important property of honesty. The honesty of a node can be calculated using Equation (3):

$$FH_{xy}(t) = \alpha_1 \text{Honesty}_{xy}^{TC}(t) + \alpha_2 \text{Honesty}_{xy}^{cen}(t) + \alpha_3 \text{Honesty}_{xy}^{coi}(t) \quad (3)$$

where FH is the final honesty and $(\alpha_1, \alpha_2, \alpha_3)$ are selected randomly, with the total honesty being equal to 1.

3.3. Routing Defense Mechanism using Evolutionary Game Theory

For various routing threats on DTNs, an RDMEG (Routing Defense Mechanism Using Evolutionary Game Theory) is described in [57]. The defense technique applies to a variety of routing systems, and focuses on information about the routing procedure that is learned through forwarded packets and acknowledgment (ACK). Evolutionary game theory is used in conjunction with the defense mechanism to evaluate and facilitate network node adaptation of the strategy. The networks are secured against intrusion and consistent transmission service is maintained using game theory. Under certain conditions, networks can reach evolutionary strategy stability (ESS) after development. The initial fraction

of nodes using different strategies only affects the game mechanism, whereas the initial parameters affect both the convergence rate and the final ESS. The proposed scheme finally computes each node's total participation value. Here, P_v is a symbol for the sum of each node's participation value, and is provided in Equation (4).

$$P_v = \alpha P_r + \beta P_a \quad (4)$$

In this case, P_r and P_a stand for the participation values acquired from forwarding and acknowledging messages, respectively, while α and β are the weight coefficients.

3.4. Collaborative Trust Management Scheme

The Collaborative Trust Management Scheme (CTMS) [58] is based on the typical MANET *watchdog technique*, which examines traffic on the network and identifies nodes behaving inappropriately. By counting the packets that each node must receive and computing a trust level for each neighbor node as the ratio of packets forwarded to the ratio of packets relayed to it, a simple watchdog deployment able to run in a node monitors the messages transferred and received by the neighboring nodes. A node's trust level is set to 1 after it transmits all of the messages passed to it. A node is labeled as malicious if its trust level is lower than the predetermined threshold. This method is classified using two phases, called the probe phase and the decision phase. Taking into account the contact history, both direct and indirect interactions are analyzed in the probe phase. The source node $IDi = src$ sends a message to node $IDdst$ and the message is stored in a relay node IDj , which then follows a specific forwarding procedure to relay the message to the next hop. The authors refer to this as their direct encounter record, which contains $\alpha(CH_{Direct}^{i \rightarrow j})$. In order for the forwarding evidence from nodes i to j to be displayed, the encounter record must be created. A record is created for each direct meeting as α and β . An expression for the direct encounter record is provided in Equations (5) and (6):

$$\alpha(CH_{Direct}^{i \rightarrow j}) = \left[IDi(src), IDj, IDdst, Mttl, Ej, Tenc \right] \quad (5)$$

$$\beta(CH_{Direct}^{j \rightarrow i}) = \left[IDj = src, IDi, IDdst, Mttl, Ej, Tenc \right] \quad (6)$$

where $IDi = src$ is the source node, IDj is the relay node, $IDdst$ is the destination node for message transmission, $Mttl$ is the packet expiry time, Ej is the average amount of energy left in IDj , and $Tenc$ is the time stamp and sequence number at the moment of contact. To update each other's encounter records, information from nodes encountered by $IDi = src$ and $[IDj = src]$ is used. These data are categorized as indirect reputations δ , which show how much faith a node has in data resulting from such a node encountered within the same network. As indicated in Equations (7) and (8), the authors employ a beta function to determine a node's level of trustworthiness in order to assess its probability of engaging in malicious activity:

$$\alpha(CH_{Direct}^{i \rightarrow j})^t = \frac{\alpha(CH_{Direct}^{i \rightarrow j}) + \delta.means(\alpha(CH_{Direct}^{j \rightarrow k}))}{2} \quad (7)$$

$$\beta(CH_{Direct}^{i \rightarrow j})^t = \frac{\beta(CH_{Direct}^{i \rightarrow j}) + \delta.means(\beta(CH_{Direct}^{j \rightarrow k}))}{2} \quad (8)$$

where $(CH_{Direct}^{i \rightarrow j})$ is the value α computed for every neighbor j of i obtained from direct encounter records at i , $(CH_{Direct}^{j \rightarrow k})$ is the value for every encountered node by j of i that is achieved from the encounter records of k by j , and δ is the degree of truthfulness from indirect interactions. The CTMS determines whether a node is acting incorrectly

after obtaining the reputation for each node and calculating the ratio between $(CH_{Direct}^{i \rightarrow j})^t$ and $(CH_{Direct}^{j \rightarrow i})^t$.

The decision module adjusts the reputation score based on the predefined threshold after the reputation value has been collected from the encounter nodes to recognize misbehaving nodes. The decisions made by the suggested collaborative trust model rely on the node's modified reputation value. A detected node is prohibited and labeled as harmful if its reputation value falls below the threshold limit. Node i updates information about node j to other encountered nodes throughout the network if node i meets node j and identifies node j as a malicious node.

3.5. Incentive and Punishment Scheme for Internet of Vehicles

An innovative mechanism named Incentive and Punishment Scheme (IPS) was proposed in [59], where vehicles with greater weights and cooperation values are elected as heads throughout the election process. The weights of these heads is been examined using the Vickrey, Clarke, and Groves (VCG) model. By actively participating, a vehicle can strengthen its incentives (reputation) in the electoral process (forwarding data). Vehicles that exhibit selfish behavior repeatedly are fined. After the election process, the monitoring nodes maintain a close watch on their neighboring nodes' performance. For the election, monitoring, and rewarding procedures, the authors created a mathematical model and algorithms. Incentives can be awarded to each node participating in the routing process as provided in Equation (9):

$$P_m(x) = \sum_{k \in n} (Vt_x(W, k)) \times (F_b) \times (\Psi_x) \quad (9)$$

where, in the election scheme, $(Vt_x(W, k))$ generates a specific value: 1 if k voted x , or 0 otherwise. The fixed budget for each election node is F_b , and the node payment is Ψ_x .

3.6. Active Trust Verification Data Collection Framework

The Active Trust Verification Data Collection (ATVDC) approach was designed for efficient, affordable, and trustworthy data collection [60]. In this method, an unmanned aerial vehicle (UAV) is used to collect baseline sensor data to evaluate how trustworthy MVs are, and a high-trust MV priority recruitment (HTMPR) strategy is recommended to swiftly and cheaply discover reliable MVs. A genetic algorithm-based trajectory planning (GATP) method is proposed to allow the UAV to collect more baseline data at the lowest flying cost, along with a plan for including MVs with a high level of trust at an affordable price. High levels of trust encourage MVs to report data honestly, which raises the accuracy of data collection. The two distinct categories of collectors, UAVs and MVs, are responsible for the ATVDC scheme's costs. As they move across the city, the MVs regularly gather data from sensors that are within transmission range. Depending on how many data packets are gathered in this manner, the data center assigns prizes. The data collected by the UAV are considered reliable, and are provided in Equation (10).

$$C_{i,j}^k = \frac{\sum (D_j \odot d_{i,j})}{512} \quad (10)$$

Here, both $D_j, d_{i,j}$ are binary values that correspond to the data value detected by the UAV at sensor s_j and the data value gathered by MV vi at sensor s_j , respectively. The size of each packet is 512 bits. The calculation's formula can be found in Equation (11), where $d_{r,j}$ stands for the information provided by a reliable MV vr at sensor s_j and $d_{i,j}$ stands for the information provided by the MV vi being evaluated.

$$\mathfrak{S}_{i,j,r}^k = \frac{\sum(D_{r,j} \odot d_{i,j})}{512} \quad (11)$$

A summary of the six IoT-based cooperation strategies described above is presented in Table 1.

Table 1. Summary of IoT-based VDTN schemes.

Scheme	Contributions	Strengths	Weaknesses
SOS [56]	Election scheme based on weight to handle the issue of selfishness	Alternate cooperation criteria	Monitoring nodes can be selfish
HBDS [10]	Election scheme based on honesty to solve the problem of selfishness	Incentive differentiation and normal punishment	Each node needs to use its memory to maintain the reputation file
CTMS [58]	Trust-based scheme is used to address the issue of selfishness	Efficient watchdog system	Due to the higher threshold reputation, nodes may be expelled from the network if they are not qualified
RDMEG [57]	Game theory scheme for motivating nodes to cooperate	Optimal decision-making	No incentive differentiation
IPS [59]	Incentive scheme for encouraging selfish nodes to cooperate	Efficient monitoring system	Ignores the selfish behaviors such as plotting, scheming, deception, self-interest, etc
ATVDC [60]	Trust-based scheme to handle the selfishness problem	Lower cost while gathering more data	Exchange of information between nodes can lead to leakage of private information

4. Simulation Settings

An NS-2 network simulator was used for the simulations [61]. The NS-2 simulator is a program that simulates discrete network activities, including packet transmitting, receiving, forwarding, and discarding. Ad hoc wireless network simulation is supported by the most recent version, ns-allinone-2.34. NS-2 is written in the Object Tool Common Language and C++ programming languages (OTCL).

For one cluster, the simulation area was approximately $4000 \times 3000 \text{ m}^2$. The network was divided into four clusters. There were 150 nodes altogether in the simulated scenario (100 terminal nodes and 50 relayed nodes). The simulation time was 48 hours for the simulation scenario. Node activities were not required to evolve. A packet's Time-to-Live (TTL) parameter was set to 350 min, and each message could vary between 100 and 650 KB in size. Two nodes typically communicate with one another at a particular instant in a specific range. At a fixed transmission range of 500 m, the interaction range between the nodes was 10 m, meaning that there was two-way communication between the nodes. The time interval for packet generation was [30, 40] s. The node communication standard was IEEE 802.11a. The buffer capacity of the terminal node was 200 MB and the relay node buffer capacity was 300 MB. The number of cooperative nodes incorporated in the scenarios was 10, 20, 30, and 40, respectively.

To assess the effectiveness of the nodes in a particular area, three types of mobility models can be employed: heavy traffic, medium traffic, and light traffic. In the heavy traffic mobility model, the nodes travel over a wider region and are more densely packed. In comparison to the other two mobility models, the light traffic mobility model has a lower density and a smaller mobility area. The medium mobility model has a medium amount of traffic. Using the parameters listed in Table 2, we employed a medium mobility model for the simulation.

Table 2. Simulation parameters and their values.

Parameters	Values
Simulation Area	5000 × 4000 m ²
Number of nodes	150
Transmission Range	500 m
Comparison	SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC
Simulation Time	48 h
Number of Relay Nodes	50
Number of Terminal Nodes	100
Terminal Nodes Buffer Capacity	200 MB
Relay Node Buffer Capacity	300 MB
Average Speed	80 km/h
Number of Cooperative Nodes	10, 20, 30, 40
Interval for Packets Generation	[30, 40] s
Node Communication	IEEE 802.11a
Size of Packets	[100, 650 KB]
Packets TTL	350 min

4.1. Performance Metrics

The following performance metrics were used to compare the performance of all frameworks used in this article. Packet Delivery Probability (PDR) is the ratio between the number of unique packets (i.e., not including packet copies) that have arrived at the final destination node(s) and the total number of unique bundles that were formed at the originating node. The Packet Delivery Delay (PDD) is the average amount of time needed for a message to travel from source to destination across the network. Average Energy Consumption is calculated as the sum of the energy used by each node to the overall number of nodes present. The Packets Dropped ratio is defined as the ratio between the number of dropped packets and the total number of sent packets. The overhead ratio determines how efficiently a system utilizes the bandwidth, and additionally determines how much space, time, and other resources are needed to finish a certain task. Finally, the throughput is the amount of successfully delivered packets between two points within a predetermined period.

4.2. Results and Discussions

This portion highlights the performance analysis of the findings from the experiments carried out using the scenario stated previously. Figure 2 shows the results obtained for packet delivery probability for all six IoT-based VDTN schemes namely, SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC. When the number of cooperative nodes is 20, the packet delivery probability of SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 40%, 37%, 34%, 29%, 17%, and 15%, respectively. The SOS scheme boosts network performance compared with HBDS, CTMS, RDMEG, IPS, and ATVDC by almost 4%, 8%, 14%, 29%, and 32%, respectively. This is due to the messages in SOS being forwarded based on the nodes' contact history and willingness level, which are completely ignored by the other schemes.

In addition, when the number of cooperative nodes is 40, the packet delivery probability of SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 76%, 62%, 58%, 50%, 31%, and 27%, respectively. Again the SOS scheme boosts network performance when compared with HBDS, CTMS, RDMEG, IPS, and ATVDC, this time by almost 18%, 23%, 33%, 56%, and 61%, respectively. Therefore, it is the observed case that the SOS scheme outperforms all five other schemes in terms of packet delivery probability. This occurs because there are more contact possibilities available to nodes throughout the simulation time, enabling them to send more packets.

Figure 3 shows the results obtained for packet delivery delay for all six IoT-Based VDTN schemes, namely, SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC. When the number of cooperative nodes is 20, the packet delivery delay of SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 320 min, 270 min, 264 min, 280 min, 290 min, and 200 min, respectively. In

this case, ATVDC scheme boosts the network performance, delivering packets 30 min, 17 min, 16 min, 20 min, and 22 minutes sooner, respectively, than SOS, HBDS, CTMS, RDMEG, and IPS. In addition, when the number of cooperative nodes is 40, the packet delivery delay of SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 140 min, 120 min, 110 min, 120 min, 180 min, and 80 min more, respectively.

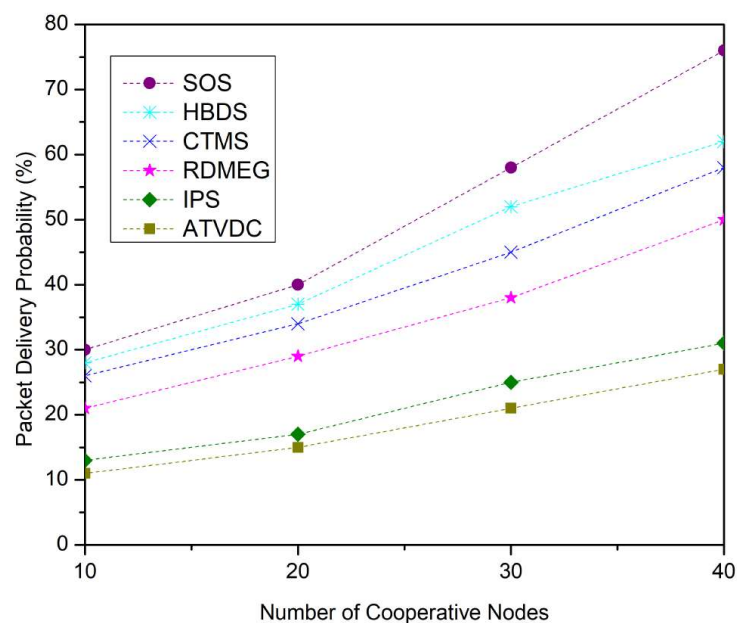


Figure 2. Packet Delivery Probability as a function of the number of cooperative nodes for the SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC schemes.

Again, the ATVDC delivers the packets 15 min, 10 min, 7 min, 10 min, and 25 min sooner, respectively, than SOS, HBDS, CTMS, RDMEG, and IPS. Therefore, it is observed that the ATVDC scheme outperforms all other five schemes in terms of packet delivery delay. This occurs because when the percentage of contact opportunities is decreases the packet delivery delay tends to be reduced, as can be seen in Figure 3.

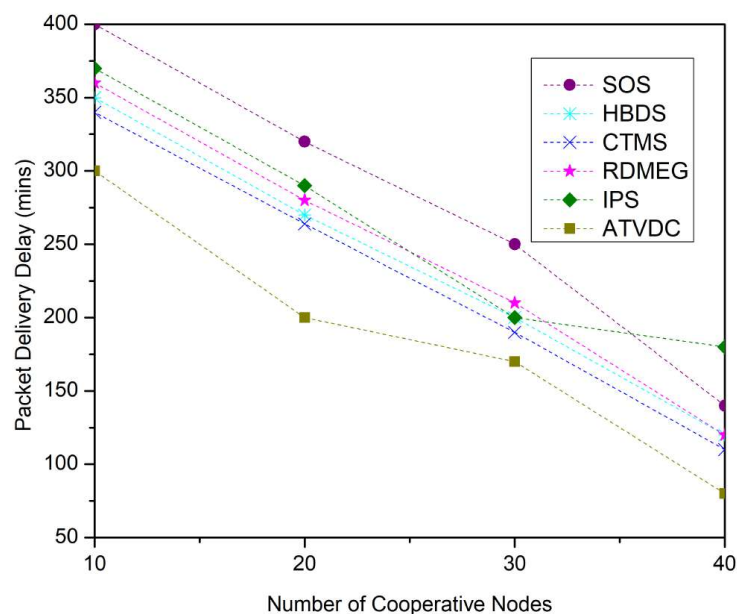


Figure 3. Packet Delivery Delay as a function of the number of cooperative nodes for the SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC schemes.

Figure 4 shows the outcomes obtained for throughput for all six IoT-Based VDTN schemes, namely, SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC. When the number of cooperative nodes is 20, the throughput of SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 240 kbps, 200 kbps, 175 kbps, 165 kbps, 160 kbps, and 145 kbps, respectively. The SOS scheme boosts network performance compared to HBDS, CTMS, RDMEG, IPS, and ATVDC by almost 14%, 22%, 25%, 27%, and 31%, respectively.

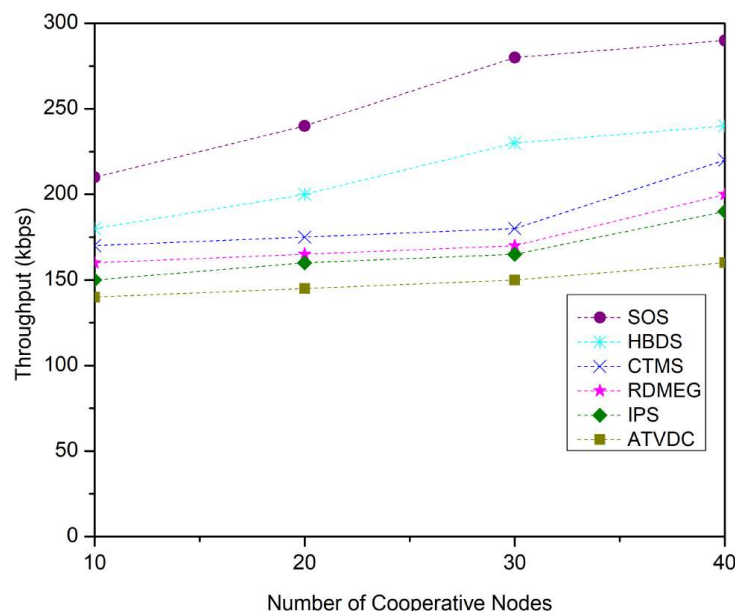


Figure 4. Throughput as a function of the number of cooperative nodes for the SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC schemes.

Similarly, when the number of cooperative nodes is 40, the throughput is 290 kbps, 240 kbps, 220 kbps, 200 kbps, 190 kbps, and 160 kbps, respectively. The SOS scheme boosts network performance compared to HBDS, CTMS, RDMEG, IPS, and ATVDC by almost 16%, 22%, 29%, 32%, and 39%, respectively. Therefore, it is observed that the SOS scheme outperforms all five other schemes in terms of throughput, as can be seen in Figure 4. This is because maintaining a constant percentage of node cooperation improves the performance of the network by preventing protocol deviation.

Figure 5 shows the outcomes obtained for energy consumption for all six IoT-Based VDTN schemes, namely, SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC. When the number of cooperative nodes is 20, the energy consumption of SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 38 Joules, 65 Joules, 67 Joules, 73 Joules, 75 Joules, and 50 Joules, respectively. Again, the SOS scheme boosts network performance compared to HBDS, CTMS, RDMEG, IPS, and ATVDC. The energy consumption of SOS is almost 30%, 32%, 39%, 41%, and 13% lower than HBDS, CTMS, RDMEG, IPS, and ATVDC, respectively. Similarly, when the number of cooperative nodes is 40, the energy consumption for SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 10 Joules, 30 Joules, 38 Joules, 45 Joules, 50 Joules, and 37 Joules respectively.

In this case, the energy consumption of SOS is almost 22%, 31%, 39%, 44%, and 30% lower than HBDS, CTMS, RDMEG, IPS, and ATVDC, respectively. Therefore, it is observed that the SOS scheme outperforms all other five schemes in terms of throughput, as can be seen in Figure 5. This is because maintaining a constant percentage of node cooperation improves the performance of the network by preventing protocol deviation. Additionally, the SOS technique encourages the network's selfish nodes to participate in the network and efficiently forward the messages.

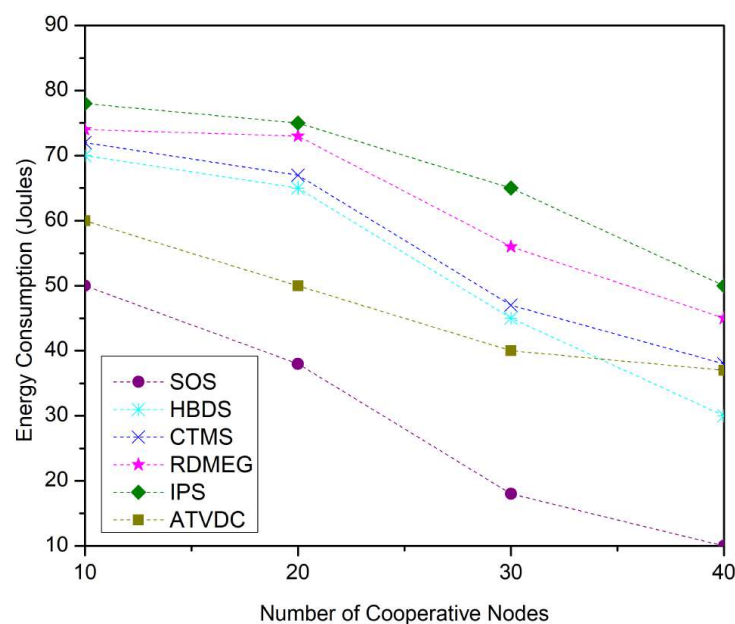


Figure 5. Energy Consumption as a function of the number of cooperative nodes for the SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC schemes.

Figure 6 shows the outcomes obtained for the number of packets dropped for all six IoT-Based VDTN schemes, namely, SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC. When the number of cooperative nodes is 20, the number of dropped packets for SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 300, 600, 700, 900, 1300, and 1700, respectively. Again, the SOS scheme boosts network performance compared to HBDS, CTMS, RDMEG, IPS, and ATVDC. The number of packets dropped by SOS is almost 15%, 20%, 30%, 50%, and 70% lower than HBDS, CTMS, RDMEG, IPS, and ATVDC, respectively. Similarly, when the number of cooperative nodes is 40, the number of packets dropped for SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 120, 400, 500, 600, 800, and 1100, respectively.

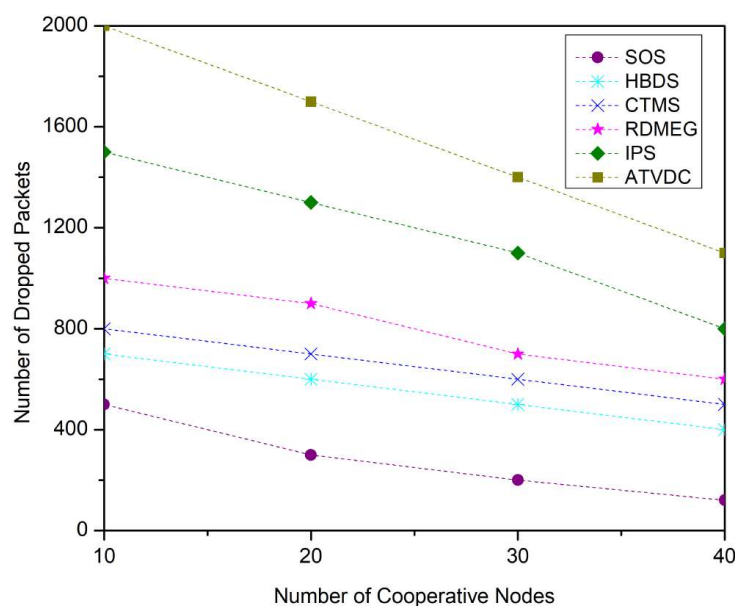


Figure 6. Number of Packets Dropped as a function of the number of cooperative nodes for the SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC schemes.

Again, the number of packets dropped by SOS is almost 14%, 19%, 24%, 34%, and 49% lower than HBDS, CTMS, RDMEG, IPS, and ATVDC, respectively. Therefore, it is observed

that the SOS scheme outperforms all other five schemes in terms of the number of packets dropped, as can be seen in Figure 6. As nodes must maintain their cooperative behavior in order to not deviate from the protocol, buffer congestion caused by keeping packets on node buffers for a prolonged period increases the percentage of dropped packets in the HBDS, CTMS, RDMEG, IPS, and ATVDC schemes.

Figure 7 shows the outcomes obtained for overhead ratio for all six IoT-Based VDTN schemes, namely, SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC. When the number of cooperative nodes is 20, the overhead ratio of SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 28, 35, 33, 55, 60, and 63, respectively. Again, the SOS scheme boosts the network performance when compared with HBDS, CTMS, RDMEG, IPS, and ATVDC. The overhead ratio of SOS is almost 8%, 6%, 33%, 40%, and 43% lower than HBDS, CTMS, RDMEG, IPS, and ATVDC, respectively. Similarly, when the number of cooperative nodes is 40, the overhead ratio for SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC is 12, 18, 30, 45, 50, and 51, respectively.

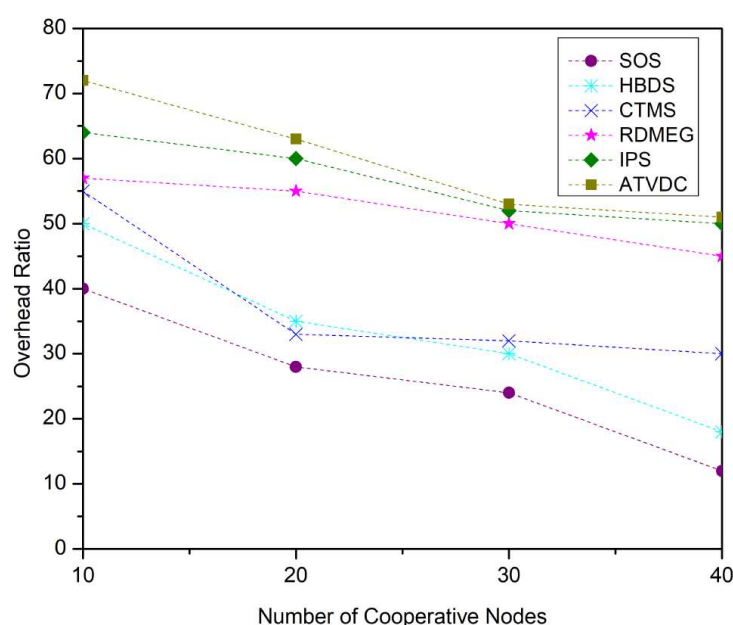


Figure 7. Overhead Ratio as a function of the number of cooperative nodes for the SOS, HBDS, CTMS, RDMEG, IPS, and ATVDC schemes.

Again, the overhead ratio of SOS is almost 7%, 22%, 41%, 47%, and 48% lower than HBDS, CTMS, RDMEG, IPS, and ATVDC, respectively. Therefore, it is observed that the SOS scheme outperforms all five other schemes in terms of overhead ratio, as can be seen in Figure 7. The existence of selfish nodes in the network significantly affects the routing procedure, in addition to affecting other nodes. Figure 7 shows details of the bandwidth performance of the routing methods and depicts the overhead. It is obvious that the overhead increases as the number of selfish nodes rises, which in turn lowers network performance.

5. Conclusions and Future Works

To implement vehicular communications in difficult contexts, such as in remote and sparsely populated areas, a recent concept called IoT-Based VDTNs attempts to overcome the most difficult problems with vehicular communications. However, due to inconsistent and intermittent communication, or even the lack of an end-to-end path between the source and destination nodes, VDTNs continue to face distinct challenges with data transfers. Cooperation strategies that encourage nodes to transfer packets during a contact opportunity must be taken into account in order to distribute packets. This article has focused on the node cooperation issue and presented six different policies for VDTNs. After reviewing the relevant literature on the topic, a comparison study was used to assess

the performance of different IoT-based VDTNs schemes in terms of several performance parameters, including packet delivery probability, packet delivery delay, overhead ratio, energy consumption, throughput, and number of packets dropped. The SOS strategy, which encourages nodes to cooperate regularly at the same percentage, was found to outperform five other proposed schemes.

This study can serve as the foundation for the creation of novel cooperative strategies, such as a cooperative system that rewards nodes for sharing their resources with other nodes that need them. It is recommended that further research be carried out in this area in the future.

Author Contributions: This work was carried out in collaboration between all authors. G.U.R., W.H.F.A. and M.Z. designed the detailed methodology. N.A.B. and Z.M. managed the literature search and detailed analysis. H.F. and J.H. wrote the first draft of the manuscript in consultation with G.U.R. The final draft of the paper was written by W.H.F.A. along with M.Z. The funding acquisition was achieved by Z.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: This manuscript has no associated data.

Acknowledgments: Special thanks to College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait for all their support in funding this project.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Piran, M.J.; Verma, S.; Menon, V.G.; Suh, D.Y. Energy-efficient transmission range optimization model for wsn-based internet of things. *Comput. Mater. Contin.* **2021**, *67*, 2989–3007.
2. Awan, S.H.; Ahmed, S.; Safwan, N.; Najam, Z.; Hashim, M.Z.; Safdar, T. Role of internet of things (IoT) with blockchain technology for the development of smart farming. *J. Mech. Contin. Math. Sci.* **2019**, *14*, 170–188.
3. Rehman, G.U.; Zubair, M.; Qasim, I.; Badshah, A.; Mahmood, Z.; Aslam, M.; Jilani, S.F. EMS: Efficient Monitoring System to Detect Non-Cooperative Nodes in IoT-Based Vehicular Delay Tolerant Networks (VDTNs). *Sensors* **2023**, *23*, 99. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Radwan, N.; Farouk, M. The Growth of Internet of Things (IoT) In The Management of Healthcare Issues and Healthcare Policy Development. *Int. J. Technol. Innov. Manag. IJTIM* **2021**, *1*, 69–84. [\[CrossRef\]](#)
5. Jan, B.; Farman, H.; Khan, M.; Talha, M.; Din, I.U. Designing a smart transportation system: An internet of things and big data approach. *IEEE Wirel. Commun.* **2019**, *26*, 73–79. [\[CrossRef\]](#)
6. Farman, H.; Khan, Z.; Jan, B.; Boulila, W.; Habib, S.; Koubaa, A. Smart transportation in developing countries: An Internet-of-Things-based conceptual framework for traffic control. *Wirel. Commun. Mob. Comput.* **2022**, 8219377. [\[CrossRef\]](#)
7. Kumar, S.; Tiwari, P.; Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: A review. *J. Big Data* **2019**, *6*, 1–21. [\[CrossRef\]](#)
8. Yuehong, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13.
9. Aly, W.H.F. A New Controller Placement Technique using Colored Petri-Nets Modelling for SDNs. In Proceedings of the 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCLOUD/SocialCom/SustainCom), Exeter, UK, 17–19 December 2020; pp. 941–947.
10. Rehman, G.U.; Ghani, A.; Zubair, M.; Ghayyure, S.A.; Muhammad, S. Honesty based democratic scheme to improve community cooperation for Internet of Things based vehicular delay tolerant networks. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4191. [\[CrossRef\]](#)
11. Rehman, G.U.; Haq, M.I.U.; Zubair, M.; Mahmood, Z.; Singh, M.; Singh, D. Misbehavior of nodes in IoT based vehicular delay tolerant networks VDTNs. *Multimed. Tools Appl.* **2022**, 1–19. [\[CrossRef\]](#)
12. Magaia, N.; Mastorakis, G.; Mavromoustakis, C.; Pallis, E.; Markakis, E.K. *Intelligent Technologies for Internet of Vehicles*; Springer: Berlin/Heidelberg, Germany, 2021.
13. Mahi, M.J.N.; Chaki, S.; Ahmed, S.; Biswas, M.; Kaiser, S.; Islam, M.S.; Sookhak, M.; Barros, A.; Whaiduzzaman, M. A Review on VANET Research: Perspective of Recent Emerging Technologies. *IEEE Access* **2022**, *10*, 65760–65783. [\[CrossRef\]](#)
14. Khan, L.U.; Yaqoob, I.; Tran, N.H.; Kazmi, S.A.; Dang, T.N.; Hong, C.S. Edge-computing-enabled smart cities: A comprehensive survey. *IEEE Internet Things J.* **2020**, *7*, 10200–10232. [\[CrossRef\]](#)
15. Dey, K.C.; Rayamajhi, A.; Chowdhury, M.; Bhavsar, P.; Martin, J. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network—Performance evaluation. *Transp. Res. Part C Emerg. Technol.* **2016**, *68*, 168–184. [\[CrossRef\]](#)

16. Li, M.; Si, P.; Zhang, Y. Delay-tolerant data traffic to software-defined vehicular networks with mobile edge computing in smart city. *IEEE Trans. Veh. Technol.* **2018**, *67*, 9073–9086. [\[CrossRef\]](#)
17. Vasilakos, A.; Zhang, Y.; Spyropoulos, T. *Delay Tolerant Networks*; CRC Press: Boca Raton, FL, USA, 2016.
18. Sobin, C.; Raychoudhury, V.; Marfia, G.; Singla, A. A survey of routing and data dissemination in delay tolerant networks. *J. Netw. Comput. Appl.* **2016**, *67*, 128–146.
19. Bylykbashi, K.; Spaho, E.; Barolli, L.; Xhafa, F. Routing in a many-to-one communication scenario in a realistic VDTN. *J. High Speed Netw.* **2018**, *24*, 107–118. [\[CrossRef\]](#)
20. AlArnaout, Z.; Mostafa, N.; Alabed, S.; Aly, W.H.F.; Shdefat, A. RAPT: A Robust Attack Path Tracing Algorithm to Mitigate SYN-Flood DDoS Cyberattacks. *Sensors* **2023**, *23*, 102. [\[CrossRef\]](#)
21. Zhao, K.; Wang, R.; Burleigh, S.C.; Sabbagh, A.; Wu, W.; De Sanctis, M. Performance of bundle protocol for deep-space communications. *IEEE Trans. Aerosp. Electron. Syst.* **2016**, *52*, 2347–2361. [\[CrossRef\]](#)
22. Hentati, A.I.; Fourati, L.C. Comprehensive survey of UAVs communication networks. *Comput. Stand. Interfaces* **2020**, *72*, 103451. [\[CrossRef\]](#)
23. Sharma, M.; Kumar, P.; Tomar, R.S. Vehicular connectivity algorithm for cooperative transportation systems. *Comput. Electr. Eng.* **2022**, *102*, 108199. [\[CrossRef\]](#)
24. Raymond, J.W.; Olwal, T.O.; Kurien, A.M. Cooperative communications in machine to machine (M2M): Solutions, challenges and future work. *IEEE Access* **2018**, *6*, 9750–9766. [\[CrossRef\]](#)
25. Khan, F.; Rehman, A.U.; Yahya, A.; Jan, M.A.; Chuma, J.; Tan, Z.; Hussain, K. A quality of service-aware secured communication scheme for internet of things-based networks. *Sensors* **2019**, *19*, 4321. [\[CrossRef\]](#) [\[PubMed\]](#)
26. Obaidat, M.; Khodjaeva, M.; Holst, J.; Ben Zid, M. Security and privacy challenges in vehicular ad hoc networks. In *Connected Vehicles in the Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 223–251.
27. Alaslani, M.; Nawab, F.; Shihada, B. Blockchain in IoT systems: End-to-end delay evaluation. *IEEE Internet Things J.* **2019**, *6*, 8332–8344. [\[CrossRef\]](#)
28. Long, N.B.; Tran-Dang, H.; Kim, D.S. Energy-aware real-time routing for large-scale industrial internet of things. *IEEE Internet Things J.* **2018**, *5*, 2190–2199. [\[CrossRef\]](#)
29. Ge, Y.; Nan, Y.; Guo, X. Maximizing network throughput by cooperative reinforcement learning in clustered solar-powered wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2021**, *17*, 15501477211007411. [\[CrossRef\]](#)
30. Felemban, M.; Felemban, E.; Kobes, J.; Ghafoor, A. Threat management in data-centric IoT-based collaborative systems. *ACM Trans. Internet Technol. TOIT* **2019**, *19*, 1–19. [\[CrossRef\]](#)
31. Ijamaru, G.K.; Ang, L.M.; Seng, K.P. Transformation from IoT to IoV for waste management in smart cities. *J. Netw. Comput. Appl.* **2022**, *204*, 103393. [\[CrossRef\]](#)
32. Dias, J.A.; Rodrigues, J.J.; Kumar, N.; Saleem, K. Cooperation strategies for vehicular delay-tolerant networks. *IEEE Commun. Mag.* **2015**, *53*, 88–94. [\[CrossRef\]](#)
33. Machado, C.; Westphall, C.M. Blockchain incentivized data forwarding in MANETs: Strategies and challenges. *Ad Hoc Netw.* **2021**, *110*, 102321. [\[CrossRef\]](#)
34. Rehman, G.U.; Ghani, A.; Muhammad, S.; Singh, M.; Singh, D. Selfishness in vehicular delay-tolerant networks: A review. *Sensors* **2020**, *20*, 3000. [\[CrossRef\]](#)
35. Magaia, N.; Sheng, Z. ReFloV: A novel reputation framework for information-centric vehicular applications. *IEEE Trans. Veh. Technol.* **2018**, *68*, 1810–1823. [\[CrossRef\]](#)
36. Dias, J.A.F.F. Performance of Management Solutions and Cooperation Approaches for Vehicular Delay-Tolerant Networks. Ph.D. Thesis, Universidade da Beira Interior, Covilhã, Portugal, 2017.
37. Yan, L.; Shen, H.; Chen, K. MobiT: A distributed and congestion-resilient trajectory based routing algorithm for vehicular delay tolerant networks. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA, 18–21 April 2017; pp. 209–214.
38. Dias, J.A.; Rodrigues, J.J.; Xia, F.; Mavromoustakis, C.X. A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks. *IEEE Trans. Ind. Electron.* **2015**, *62*, 7929–7937. [\[CrossRef\]](#)
39. Magaia, N.; Borrego, C.; Pereira, P.R.; Correia, M. ePRIVO: An enhanced privacy-preserving opportunistic routing protocol for vehicular delay-tolerant networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11154–11168. [\[CrossRef\]](#)
40. Benamar, N.; Singh, K.D.; Benamar, M.; El Ouadghiri, D.; Bonnin, J.M. Routing protocols in vehicular delay tolerant networks: A comprehensive survey. *Comput. Commun.* **2014**, *48*, 141–158. [\[CrossRef\]](#)
41. Park, Y.; Sur, C.; Rhee, K.H. A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency. *Secur. Commun. Netw.* **2018**, *2018*, 5932183. [\[CrossRef\]](#)
42. Triadi, M.B.; Perdana, D.; Munadi, R.; Wenzao, L. A new variant of game theory based decision making (GTDM) algorithm routing protocols to improve energy efficiency on vehicular delay tolerant network (VDTN). *Int. J. Commun. Netw. Inf. Secur.* **2019**, *11*, 224–231. [\[CrossRef\]](#)
43. Ogah, C.P.A. *Security and Privacy in VANET-Based Intelligent Transport Systems (ITS)*; University of Surrey: Guildford, UK, 2018.
44. Loudari, S.; Abouhassane, A.; Benamar, N.; Younis, M. DASH: A Distributed Approach for Selfishness Handling in a DTN. In Proceedings of the 2019 2nd IEEE Middle East and North Africa COMMUNICATIONS Conference (MENACOMM), Manama, Kingdom of Bahrain, 19–21 November 2019; pp. 1–6.

45. Ye, F.; Chen, C.; Zheng, Z. Deep autoencoder-like nonnegative matrix factorization for community detection. In Proceedings of the 27th ACM International Conference on Information and Knowledge Management, Turin, Italy, 22–26 October 2018; pp. 1393–1402.
46. Ning, Z.; Liu, L.; Xia, F.; Jedari, B.; Lee, I.; Zhang, W. CAIS: A copy adjustable incentive scheme in community-based socially aware networking. *IEEE Trans. Veh. Technol.* **2016**, *66*, 3406–3419. [\[CrossRef\]](#)
47. Jain, S.; Verma, A. Bubble rap incentive scheme for prevention of node selfishness in delay-tolerant networks. In *Smart Innovations in Communication and Computational Sciences*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 289–303.
48. Hasani, H.; Babaie, S. Selfish node detection in ad hoc networks based on fuzzy logic. *Neural Comput. Appl.* **2019**, *31*, 6079–6090. [\[CrossRef\]](#)
49. Jedari, B.; Liu, L.; Qiu, T.; Rahim, A.; Xia, F. A game-theoretic incentive scheme for social-aware routing in selfish mobile social networks. *Future Gener. Comput. Syst.* **2017**, *70*, 178–190. [\[CrossRef\]](#)
50. Guo, Y.; Zhang, H.; Zhang, L.; Fang, L.; Li, F. Incentive mechanism for cooperative intrusion detection: An evolutionary game approach. In *International Conference on Computational Science*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 83–97.
51. Haq, A.; Faheem, Y. A peer-to-peer communication based content distribution protocol for incentive-aware delay tolerant networks. *Wirel. Netw.* **2020**, *26*, 583–601. [\[CrossRef\]](#)
52. Sharma, A.; Goyal, N.; Guleria, K. Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes. *J. Supercomput.* **2021**, *77*, 6036–6055. [\[CrossRef\]](#)
53. Jethawa, H.; Madria, S. Reputation and credit based incentive mechanism for data-centric message delivery in DTNs. In Proceedings of the 2018 19th IEEE International Conference on Mobile Data Management (MDM), Aalborg, Denmark 26–28 June 2018; pp. 207–216.
54. Dias, J.A.; Rodrigues, J.J.; Kumar, N.; Mavromoustakis, C.X. A hybrid system to stimulate selfish nodes to cooperate in vehicular delay-tolerant networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 5910–5915.
55. Available online: https://www.researchgate.net/figure/The-Internet-of-Vehicles-scenario_fig1_310734157 (accessed on 12 December 2022).
56. Rehman, G.U.; Ghani, A.; Zubair, M.; Saeed, M.I.; Singh, D. SOS: Socially omitting selfishness in IoT for smart and connected communities. *Int. J. Commun. Syst.* **2023**, *36*, e4455. [\[CrossRef\]](#)
57. Guo, H.; Wang, X.; Cheng, H.; Huang, M. A routing defense mechanism using evolutionary game theory for delay tolerant networks. *Appl. Soft Comput.* **2016**, *38*, 469–476. [\[CrossRef\]](#)
58. Asuquo, P.; Cruickshank, H.; Ogah, C.P.A.; Lei, A.; Sun, Z. A collaborative trust management scheme for emergency communication using delay tolerant networks. In Proceedings of the 2016 8th Advanced Satellite Multimedia Systems Conference and the 14th Signal Processing for Space Communications Workshop (ASMS/SPSC), Palma de Mallorca, Spain, 5–7 September 2016; pp. 1–6.
59. Rehman, G.U.; Ghani, A.; Zubair, M.; Naqvi, S.H.A.; Singh, D.; Muhammad, S. Ips: Incentive and punishment scheme for omitting selfishness in the internet of vehicles (ioV). *IEEE Access* **2019**, *7*, 109026–109037. [\[CrossRef\]](#)
60. Huang, S.; Gui, J.; Wang, T.; Li, X. Joint mobile vehicle-UAV scheme for secure data collection in a smart city. *Ann. Telecommun.* **2021**, *76*, 559–580. [\[CrossRef\]](#)
61. Fakhar, F. Investigate Network Simulation Tools in designing and managing intelligent systems. *J. Inf. Syst. Telecommun.* **2019**, *7*, 278–293.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.