Computers, Materials & Continua
DOI:10.32604/cmc.2022.021374
Article

Tech Science Press

Incentive-Driven Approach for Misbehavior Avoidance in Vehicular Networks

Shahid Sultan[1], Qaisar Javaid[1], Eid Rehman[2,*], Ahmad Aziz Alahmadi[3], Nasim Ullah[3] and Wakeel Khan[4]

[1]Department of Computer Science and Software Engineering, International Islamic University, Islamabad, 44000, Pakistan
[2]Department of Software Engineering, Foundation University Islamabad, 44000, Pakistan
[3]Department of Electrical Engineering, Taif University KSA Taif, 21944, Saudi Arabia
[4]Department of Electrical Engineering, Foundation University Islamabad, 44000, Pakistan
[*]Corresponding Author: Eid Rehman. Email: eid.rehman@fui.edu.pk
Received: 01 July 2021; Accepted: 20 August 2021

Abstract: For efficient and robust information exchange in the vehicular ad-hoc network, a secure and trusted incentive reward is needed to avoid and reduce the intensity of misbehaving nodes and congestion especially in the case where the periodic beacons exploit the channel. In addition, we cannot be sure that all vehicular nodes eagerly share their communication assets to the system for message dissemination without any rewards. Unfortunately, there may be some misbehaving nodes and due to their selfish and greedy approach, these nodes may not help others on the network. To deal with this challenge, trust-based misbehavior avoidance schemes are generally reflected as the capable resolution. In this paper, we employed a fair incentive mechanism for cooperation aware vehicular communication systems. In order to deploy a comprehensive credit based rewarding scheme, the proposed reward-based scheme fully depends on secure and reliable cryptographic procedures. In order to achieve the security goals, we used the cryptographic scheme to generate a certified public key for the authenticity of every message exchange over the network. We evaluated the friction of misbehaving vehicles and the effect of rewarding schemes in context with honest messages dissemination over the network.

Keywords: VANET; misbehavior; reputation; rewards; congestion avoidance; certified public key

1 Introduction

The emergence of Vehicle Ad Hoc Network (VANET) brings new challenges and requires deeper Consideration about vehicle reputation and trust calculation because these parameters can be used to accept or forward the message over the network. Incentive schemes for cooperative VANET frameworks can be characterized as trust and credit-based schemes. A comprehensive trust management system allows vehicles to interact in the network based on the assessment and evaluation of past historical communication. To preserve the reputation history of other vehicles is a challenging task as most of the vehicles are anonymous and changing their identities

periodically. It is also very difficult to store trust and reputation information for a dense and large-scale network. An adaptable and general-purpose trust-management approach can keep up-to-date and reliable data delivery with diverse entities in a distributed network [1].

In addition, since VANETs are independent and self-organizing systems of participation between vehicles, we cannot continuously anticipate all vehicles to intentionally contribute their computing assets to the network. Additionally, a few selfish vehicles will not forward message hand-off services for other vehicles. One way to resolve this challenge is to back motivations to compensate for deliberate cooperation within the network with credit rewards [2].

For example, when the sender requests help from the vehicle, the sender will motivate the vehicle so that the vehicle is willing to store, carry and forward the sender's message to the destination. Although, on the one hand, incentives seem to be an attractive approach to selfish behavior, another problem is how to determine whether the sender actually delivers the message to the destination. If the source location server first provides a credit line for the vehicle, the malicious vehicle will not faithfully store the message to the designated destination after receiving the credit line. The origin location server may worry about this malicious behavior of the vehicle, that is, the so-called meal and dash, which is unfair to the origin location server. Therefore, how to solve the unfair problem of the incentive scheme on the autonomous vehicle network is also a serious challenge [3].

In our proposed scheme, the vehicle can accept and exchange messages at an event time after assessing and evaluating the trust and reputation score of the participating vehicles in the network. To analyze the behavior of the particular vehicular node, the proposed scheme evaluates the type of message exchanged in each transaction in context with vehicular reputation score. The reputation of the sender vehicle that creates or forwarding the message plays a decisive role in accepting the forwarded or created message. To this approach, the vehicle's trust and reputation certificate score is assigned to the message created or forwarded by a specific vehicle. We proposed an incentive-driven approach that works with the generation of a certified public key for robust and secure dissemination over the network. In the proposed scheme, a collaborative trust mechanism is adopted for calculating the reputation and trust score for every vehicular node. Reputation and trust scores can be suitable tools for accepting and forwarding messages in correlation with two behavioral factors: use to generate event-driven messages about road conditions and to cooperate when forwarding messages. In order to achieve the security goals, we used the cryptographic scheme to generate a certified public key for the authenticity of every message exchange over the network. We evaluated the friction of misbehaving vehicles and the effect of rewarding schemes in context with honest messages dissemination over the network.

The rest of the paper is organized as follows: Section II describes work related to misbehavior avoidance in VANETs; Section III defines system model including system architecture of incentive-driven scheme, secure public key generation, and incentive paradigm; Section IV includes performance evaluation, network parameters and discussion of the results of the proposed scheme; Section V summarizes the conclusion of the research study.

2 Related Works

In this section of the paper, we emphasize on work related to trust and reputation management schemes. Second, we relate the trust-based approach to an incentive-driven mechanism.

In VANET scenario, trust and confidence building measures are the vital research areas, because vehicular nodes introduce fake information in the network system. Centralized approaches

for trust management are not best suited for large scale network; VANET requires trust-based approaches for a service provider that experiences higher network delay. A significant effort has been made to create distributed trust administration schemes for VANETs, based on the presumption that it is not conceivable to depend on a centralized approach for VANETs. The primary reason for implementing a centralized system is that the vehicles are directed and represented by a central authority. Hence, it is natural to adopt a centralized scheme [4]. In expansion, the centralized framework may be best fitted than decentralized due to simple administration, control, and security.

Nowadays, it is conceivable to structure a centralized reputation framework that includes innovations such as Long-Term Evolution (LTE); this can be the foremost effective way of linking the vehicles to the Internet. Another approach utilized a single-hop trust calculation mechanism and proposed a multi-hop implementation based on carrying and forward strategy [5]. The recommendations look to assess the reliability of messages and the accumulation of reputation scores. In any case, these schemes need protection and security since the messages and inputs are linkable and not anonymous. An intruder can launch an attack on traceability to trace out the pathway of a target vehicle. The author in [6] defined a nonexclusive reflection to authenticate the anonymous announcement mechanism utilizing the reputation framework. Trust information can be collected through neighboring participating nodes in a very short span of time. Trust-based misbehavior detection schemes assigned trust values to the node based on their past communication information [7].

The author introduced a time series pattern, RSS evaluation, and the historical communication record for a specific vehicular node and dynamic connection procedure in [8]. The mentioned scheme comprehensively evaluates the direct and indirect trust and reputation scores and quality parameters to handle intrusion attacks. The vehicular trust model based on Bayesian inference proposed in [9] works on intrusion attacks.

Chen et al. [10] presented a full depiction of a novel cryptographic primitive, which enhances the mechanism to address a secure medium for the recovery of updated cryptographic keys. The author in [11] proposed a blockchain-based anonymous reputation system (BARS), to preserve privacy the proposed mechanism disrupts the congeniality between honest nodes and public keys. The work by [12] presented a trust-based dueling deep reinforcement learning approach (T-DDRL); the network deployment includes dueling network design into a consistently centralized control system of software-defined Networks (SDN). The authors in [13] used trust-based techniques to find out vehicular location with the assistance of the trust value of the node. Kumar et al. [14] proposed an improved trust-based technique to choose trusted vehicular nodes through which messages are exchanged.

The work in [15,16] suggested a reputation-based system, where network nodes assess trust relationships with each other and vote on neighboring node's activity of message exchange so that non-cooperative nodes with low reputation scores are prohibited from the system. In order to stimulate vehicles to cooperate positively, the author in [17] proposed a robust incentive mechanism integrating with Bitcoin for Vehicular Delay tolerant Networks (VDTNs) to give rewards for their positive efforts. MultiSig transaction is used to ensure fairness of the rewarding scheme so only those vehicles redeem the Bitcoins incentive transactions provided that vehicle honestly completes the message forwarding to a target vehicle. The scheme [18] presented three primary prototypes from the fundamental model of the Internet of vehicles. On the basis of the fundamental models, the categorization and classification of the fundamental model were analyzed; and at the end, optimization impacts were compared for different variables. In [19], the

authors presented a stimulus-centric approach to credit Blockchain. The driver can get Credit coins for positive contributions provided that legendary focuses must be on the normal behavior of the participating vehicles.

However, Credit Coin portends security breaches and permits dependent offense in light of Blockchain, and traces out malicious approaches to dangerous zones in a horrendous case and so on.

The scheme [20] proposes re-broadcast operations and a credit-based incentive approach for achieving effectiveness in honest data exchange. A mechanism in [21] based on the Blockchain techniques executes a credit installment service for participating vehicles. The technique used to assist the utilization and pathway service in Vehicle-to-vehicle communication. MobiCent [22] proposes a credit-incentive approach for the Disrupt Tolerant Networks (DTNs) and calculates incentives by a multiplicative decreasing remuneration (MDR) scheme. The proposed scheme helps to minimize the computation cost and delay of the network. However, the source and target vehicle have the opportunity to access the network for exchanging messages all the time over the network. The reciprocal incentive scheme (RIS) proposed in [23] investigates how two types of malicious vehicular nodes select appropriate data sources to exploit network resources for personal profit gain under extreme buffer limitations.

Furthermore, the proposed RIS approach ignores those nodes in VANET that have different levels of benefits and maliciousness for different kinds of exchanged data. As a result, the scheme suffers a higher ratio of latency to receive the required data contents successfully. To address these defects, three types of approaches such as credit-based [24–26], reputation-based [27,28] and tit-for-tat (TFT)-based [29,30] incentive mechanisms have been proposed to motivate the vehicular nodes to share their data and resources. The mentioned schemes focused on trust and credit evaluation to stimulate the vehicular node to exchange the content data to its neighbors by disbu*RSi*ng some credit reward to it. For every message-forwarding operation, a central authority would charge the source node of the data packet a part of the credit reward and pay it to each communicated node. It is worth mentioning that the failure of the central authority becomes a major issue while paying among the participating nodes.

However, these solutions additionally need to implement a reputation management system or virtual coin management system that depends on VANET applications. Existing work does not provide analysis and experiments to calculate the packet transfer rate and transmission delay of the encryption function, as well as the number of messages that is the implementation of this scheme. In addition, the existing incentive scheme completely relies on a central and trusted third party to allocate some virtual coins to each node and track the virtual coins that have been issued in the system.

3 Proposed System Model

The main emphasis of this work is to apply a collaborative trust approach to avoid misbehavior of vehicular node in VANET ensuring less packet drop ratio and robust end-end throughput. In our proposed scheme, to avoid message congestion on highways and roads it is suggested that each node or vehicle receive a single message per node with certified key pair. To cope with the issue of duplication of messages a public key-based strategy will be followed to discard and reduced the retransmission of unnecessary packets. A vehicular node will only send and respond to the most current data based on the unique identifier associated with the specific data packet.

Congestion control schemes are mainly the procedures and techniques to keep the network load below the defined capacity of the network. In VANET flooding technique is employed to route the packets across the whole connected network. In this network topology, we have to send and receive many data packets from a node to one or multiple destinations. In flooding the routing is as simple as every packet is sent back through every outgoing link. But it is also associated with certain issues such as contention of a medium, collision of packets, and redundancy or duplication of messages.

3.1 Architecture

VANET applications can be categorized in store, carry, and forward mechanisms in collaboration with participating vehicles where source to destination cannot be linked directly. To design a certified public key scheme, we consider that a vehicle assisted in carrying some data packets received from the main server to the points for displaying the information as depicted in Fig. 1.

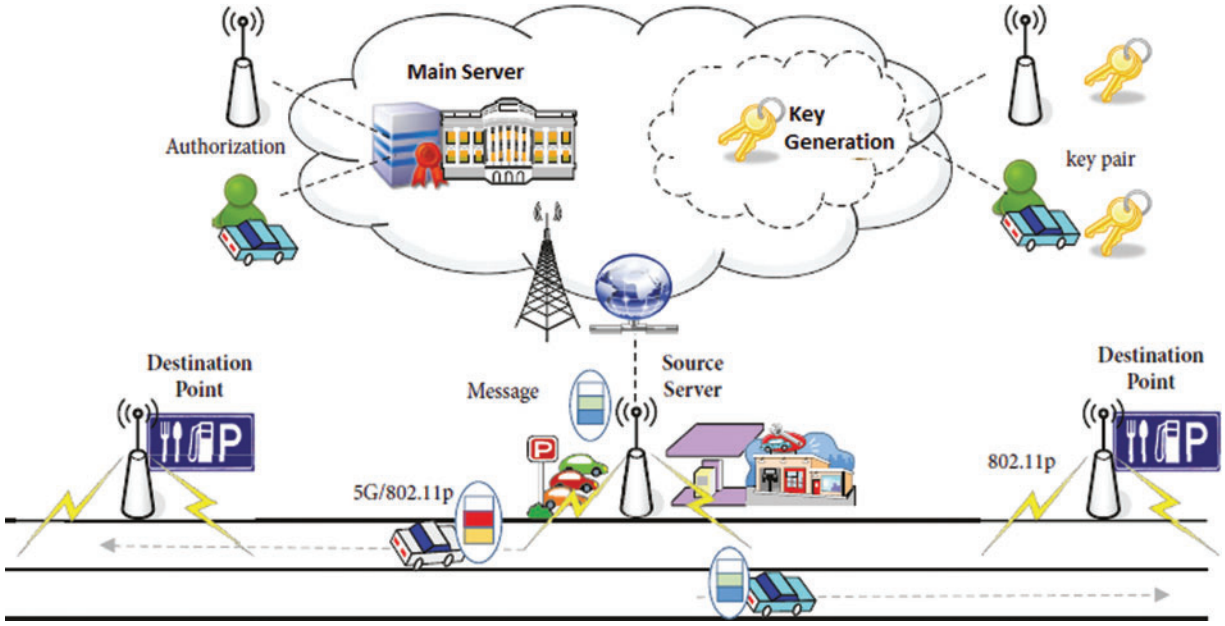

Figure 1: Public key-based Information propagation model in VANET

(i) Main Server (MS) controls Road Side Units (RSUs) and authorizes participating vehicles for message propagation services on VANETs. Authentication of vehicular nodes can be done with the process of generating certified public keys for roadside units and participating vehicles.

(ii) Participating vehicles in the network are fitted out with On Board Units (OBUs) capable of LTE/5G communication. The 802.11p standard is used for Vehicle to Infrastructure and Vehicle to Vehicle communications with a digital map navigation system.

(iii) MS is responsible for controlling RSUs with 802.11p capability for collaborating with nearby vehicles. As roadside units don't have direct communication with all participating vehicles, so indirect communication can only be possible using the opportunistic approach with the help of nearby vehicles.

We assume that roadside units and vehicles have their key pairs to receive and transmit messages. When a roadside unit or source server requests a participating vehicle to transmit a message to a specific destination vehicular point, the roadside unit or source server generates a public key pair from the main server to the participating vehicle. The roadside source server locked the key pair under the condition that these certified key pairs can be utilized by the specific participating vehicle which carries the message to the destination vehicular point. These certified key pairs can be used if the vehicle trustfully transmits the message to the destination point and receives an acknowledgment.

Algorithm 1 shows the reputation calculation of each vehicle in the proposed system. To calculate the reputation of the nodes Reputationupd function is used. RSU calls these functions and exchanges event information with nearby vehicular nodes. If the event occurrence is genuine, the reputation value of the vehicle will increase by 5 points. Otherwise, the reputation of the vehicle is reduced by 20 points. It prevents vehicles from signing and initiating false occurrences. In addition, this feature will also check the current reputation value of the vehicle to prevent signing or launching a false event. If the reputation of the vehicle is found to be less than 20, then the Central Authority (CA) cancels the registration of the vehicle by deleting it from the network. The function also describes that the reputation value has only increased to 60 points. This means that the node with the largest reputation value has only two opportunities to continuously verify the false event and then cancel its registration.

Algorithm 1 Reputation Updates

***Input**: event Id, vehicleId*
***Output**: Blacklist, emit vehicle*
Step 1: function Reputationupd (eventID, vehicleID)
*Step 2: Get values***:** *ReputationScore RS*
Step 3: if eventID == true then
if RS<70 then
RS = RS+5
else
RS unchanged //End inner if else
else
if RS<25 then
Blacklist vehicle's ID
else
RS = RS-5 //End of nested if else
Step 4: emit vehicle ID, RS
Step 5: return blacklist, emit vehicles

3.2 Security Goals

In this paper, we highlighted how to implement certified key generation scheme for VANETs in term of following security goals.

(i) *Vehicle authorization*: as VANET is monitored by Computer-based algorithm, only the vehicular nodes authorized by MS would be able to communicate over the network. Vehicle authorization process prevents illegal entities from mishandling the information propagation over the network.

(ii) *Vehicle anonymity*: hiding the identities of the source and destination points in store-carry-forwarding mechanism during VANET communication.

(iii) *Fair allocation of resources*: resources must be allocated to the participating vehicles while ensuring fairness. If a vehicle successfully transmits a message from source point to the destination point, the resources must be fairly allocated in order to prevent from dine and dash situation.

The proposed system attains these security measures by adopting certified public key mechanism for authorization of vehicles. Tab. 1 depicted the basic notations used in the proposed system.

Table 1: Notations and description

Notation	*Description*
C_{pk}	Certified public key
(K, k_{pub})	Master and public key pair of MS
V_i	Vehicle node entity i
bsk_i	Private key for entity i
bpk_i	Public key for entity i
r_i	Random number selected by MS
T_x	Instance of transaction
T_s	Time stamp
C	Cipher text
$T_X.in$	Input transaction for X
$T_X.out$	Output transaction for X
$Sign(bsk, m)$	Private key signature for message m
$Vrf(bpk, \Omega)$	Public key verification for signature Ω
Y_i	Derived public key
$M_p\ (\dot{G} \rightarrow Z_q)$	Map function of $\dot{G}$ *to* Z_q
RSi	Roadside server for entity i

3.3 Cryptographic Schemes

A symmetric encryption plot comprised of three calculations which are depicted as below.

(i) Key Generation (1^k): in this phase input for Key parameter 1^k and output parameter $1^k \in K$.
(ii) Encryption (k_{pub}, m): the second phase takes input for public key parameter k_{pub} and text m for all output ciphertext c.
(iii) Decryption (k_{pub}, c): third phase input for public key parameter k_{pub} and ciphertext c to generate output text message m.

3.4 Certified Public Key Generation

For calculating public key pair for road side units and participating vehicles, we assume that each RS_i and V_i on VANET has a master key K allotted by the Main server. Moreover, RSi have its own key pair ⟨ bskSi, bpkSi⟩ and V_i also have its own key pair ⟨bskVi, bpkVi⟩. Furthermore, let $\langle bsK_i, bpk_i, V_i, RSi \in \dot{G}\rangle$ be the public key parameters for road side server and participating

vehicle. In order to derive certified public key, let $\langle p, q, \dot{G}, P \in G\rangle$ where p and q represent prime numbers, G represent addition function and P represented base point for G.

Let $\langle K, k_{pub}\rangle$ be the master and public key allotted from MS where public key can be $k_{pub} \in \dot{G}$ and master key can be $K = P.k_{pub}$. For each vehicular entity V_i certified public key pair C_{pk} can be generated as:

(1) V chooses $bsk_i \in \dot{G}$ and then computes its master key K_i =., $k_{pub}.P$, V_i then send K_i to MS and requests for certified public key.

(2) we sssumed that the that V_i is valid and legitimate vehicle, MS selected a random number $r_i \in G$, and computes certified public key as $C_{pk} = K_i + r_i \cdot P$ and $Y_i = r_i + \rho(C_{pk}) \cdot k_{pub} \pmod q$ where ρ is a positive integer used for encoding function by element G. Now SM provides the generated certified public and derived keys $\langle C_{pk,} Y_i\rangle$ to V.

(3) V_i computes y'$_i = Y_i + k_{pub} \pmod q$, Y'i $y'_i \cdot P$ and verify that $Yi = C_{pk} + (C_{pk}) \cdot K$.

The calculated key set for $V\langle bsk_i \Leftarrow Y_i, bpk_i \Leftarrow Y'i\rangle$ can be used as public and private key pair respectively and C_{pk} can be taken as certified public key. As we calculated V_i's certified public key C_{pk}, the public key Yi can also be derive from C_{pk} through MS's public key K as $Yi = C_{pk} + (C_{pk}) \cdot K$.

The C_{pk} itself is encrypted in input and output transactions for designated the recipient of message m. in contrast, in our proposed system, the C_{pk} is only used for authentication process of the participating vehicle V_i and *RSi*.

3.5 Incentive Driven Message Forwarding and Verification

In this section of the, we discussed an incentive-based forwarding mechanism to pay the reward to the vehicle for successful message delivery across the network. In case, if *RSi* needs to send a message m to *RSj* through a store-carry-forward mechanism with the assistance of V_i. Then *RSi* demands V_i to carry out a message m to *RSj*, the system initiates an incentive transaction T_x for *RSi*. If V_i successfully finishes the message forwarding process for *RSi* then incentive transaction T_x is credited to the system network. The incentive transaction T_x can be cashed by RSj using an encashment forward signature (FwdSig) transaction.

In case, if V_i does not send the message m to RSj, *RSi* will lose its incentive. Once T_x is credited to the system, the *RSi*'s input value of T_x is termed as consumed in the incentive scheme. To handle this condition, we set time-stamp T_s condition locked with FwdSig for *RSi* to draw the incentive from T_x. This scheme is suitable in the case where V_i deliberately not forward the message earlier than the time-stamp lock condition expires. Algorithm 2 shows the function that defines the incentive mechanism for witnesses who verify the event information produced by the source node. Utilizing the define function, RSU adds the credit reward to the account of the responding vehicle and deducts the same amount from the account of the event initiator's vehicle. Another define function "emit" is used at the end to save the data in the Blockchain.

Algorithm 2: Incentive Awarding

Input:DVID, RVID, amount
Output: *emit DVID, RVID*
Step 1: function Incentives (DonorVehicleID (DVID), RecipientVehicleID (RVID), amount)
Step 2: Get values: DonorAccBalance, Recipient AccBalance
Step 3: DonorAccBalance = RecipientAccBalance
Step 4: RecipientAccBalance = RecipientAccBalance +amount
Step 5: return emit DVID, RVID, amount

The detailed proposed scheme for message forwarding and signature verification is defined as follow:

(1) The *RSi* broadcasts a request over the network system and asks for the assistance of the volunteer vehicle to carry a message m to *RS*j. The broadcast request includes the location information and identity of the *RS*j.

(2) We can assume that V_i which is near by *RS*j's location and voluntarily helps *RSi* for message forwarding, responds to *RSi* by giving $\Omega =$ Sig($bsk_i V_i$, *RS*j $\|$ loc) with its $C_{pk} V_i$.

(3) *RSi* verifies the signature Ω as v ($bpk_i V_i$, Ω) by deriving V_i's public key $bpk_i V_i$ from $C_{pk} V_i$ as calculated in Section D. After verification if the signature found valid, *RSi* formulates incentive transaction T_x1 and combines a message $msg1: = \{m \| T_s \|$ *Sig* (bsk_i *RSi*, $m \| T_s$), C_{pk} *RSi*, $T_x1\}$. Incentive transactions for crediting and reclamation amount as incentives can be stored in T_X1. where $T_X1.in$ specifies credited amount received from *RSi*'s MS pool. V_i recorded the amount given as incentives in T_X1. out and the reclamation condition for T_X1. out is described by using script-locking containing of 2-of-2 FwdSig for V_i and time-stamp constraint for *RS*j. At last, *RSi* publishes the T_X1 to the incentive network and delivers msg1 to V_i.

(4) As V_i received $msg1$, V_i calculates *RSi*'s certified public key from C_{pk} *RSi*, which is then used for the verification of *RSi*'s signature. The message is now stored and carries to the destination point RSj by vehicle V_i. Moreover, V_i initiate a validation check of T_x1 using incentive network and generates transaction T_x2 to claim the amount specified in T_x1. out. To claim the amount, Vi verify the transaction T_x2 excluding FwdSig unlocking script of transaction T_x2. in.

(5) If V_i founds to be an honest and successful volunteer vehicle, the system will allow V_i to store, carry, and forward.

(6) When V_i reaches at the target location and recognizes *RSj*, V_i constitutes another message msg2: $= \{m \| T_s \|$ si(bsk_i *RSi*, $m \| T_s$), C_{pk} *RSi*, $T_x2\}$ and exchange the same with to *RSj*.

(7) RSj analyzes the msg2 and initiates the signature verification process (bsk_i, $m \| T_s$) through $C_{pk} RSi$. After successful verification RSj accepts the message m from V_i.

(8) As to acknowledge the message delivery of V_i, *RSj* generates transaction T_x2 and generates a partial signature to unlock 2-of-2 FwdSig script. This signature can be used by V_i to spend the amount claim in the preceding transaction T_x1. out. The generated signature {Tx2, Sig (bsk_i RSj, T_x2), C_{pk} *RSj*} can be provided to V_i by *RSj*.

(9) V_i calculates *RSj*'s public key from C_{pk} *RSj* to verify the signature {Tx2, *Sig* (bsk_i *RSj*, T_x2), C_{pk} *RSj*}. If the signature is valid, V_i finalizes 2-of-2 FwdSig unlock-script by appending V_i signature with T_x2. Finally, T_x2 will be published to the incentive network to en-cash the amount given by T_x1 to V_i's account.

Algorithm 3: Signature Verification

```
Input: FwdSig, SignList, status
Ouput:SomgList, Invalide Signature
Step 1: function Vrf (FwdSig, SignList, status)
Step 2: for j= 0: j<SignList.length: j++ do
        if FwdSig == SignList[i] and status == "Verified"
            Push SignList [i] in validSignatures
        else if FwdSig == SignList[i] and status == "NotVerified"
          {
            Push SignList [i] in invalidSignatures
            else if FwdSig == SignList[i] and status == "Cancel"
            Push SignList [i] in revokedSignatures
                else return "Invalid Signature" // End of inner if else
          return emit status, FwdSig, SignPool
            } // End of for loop
```

The validation process can be started on transactions T_x1 and T_x2 over the incentive network, upon successful validation the transactions T_x1 and T_x2 will be appended to the blockchain network. As a result, V_i can get a credited amount as incentive for its volunteer cooperation for message propagation on VANETs. The most important aspect of the 2-of-2 FwdSig lock-script is that it cannot be accomplished alone by V_i. Therefore, V_i will not be rewarded if it stops message forwarding even if T_x1 is already published to its account in step 3 because V_i cannot solely achieve 2-of-2 FwdSig lock-script. As soon as *RSi* finds that T_x1 is not cashed by V_i after the time-lock expires, *RSi* freeze the transaction *TX*'2 to publish incentive because V_i did not forward the message *m* to the actual destination point *RSj*. Algorithm 3 shows the function of FwdSig, used for verification of the signatures of every vehicle. *RSi* generates a confirmed the list of verified, not verified, and cancelled signatures using this function.

4 Proposed System Model

In this section, we evaluate the implementation scenarios and elaborate to obtained experimental results in detail. Our performance evaluation objectives are three folded:

i) To motivate node contribution in the message delivery and to illustrate the requirements of the incentive scheme.

ii) To verify the practicability of the proposed incentive schemes.

iii) To investigate the special effects of different system parameters on the incentive and rewards scheme.

4.1 Simulation Setup

The simulation parameters are shown in Tab. 2. We assume that power balancing is the same for all nodes. Furthermore, we also assume that no handoffs have been taking place and there is no radio link failure detected in simulation parameters. The simulation parameters in the experimental setup are depicted in Tab. 2.

Table 2: Simulation parameters

Parameter	Value
Area	1000–1500 meters
Number of mobile nodes	18
Cluster area	r 100 m
Data packet size	1 KB
Buffer size	1 GB
Channel type	Wireless
Interface queue type	Drop tail
MAC protocol type	Mac/802-11
Propagation model	Two ray
Antenna type	Omni antenna
Vehicle in queue	10–50
Routing protocol	AODV

4.2 Experimental Results

In the proposed scheme the communication cost is measured by the ratio of transmitted byte counted at the channel, which both include event-driven data and periodic data across the networks. In congestion the medium is wholly or partially exploited by the periodic beacons thus the event-driven message could not be disseminated timely.

Figs. 2 and 3, the effects of misbehaving vehicular nodes on the performance evaluation of VANET are investigated in the situation where no incentive scheme is implemented. In the simulation scenario, a misbehaving vehicular node will only forward its self-created messages but decline to deliver those created by other vehicular nodes. Fig. 2 depicted the impact of the misbehaving vehicles on packet delivery ratio (PDR). Two lines curve in Fig. 2 illustrates the decline tendency of the PDR and relative packet delivery ratio (RPDR) as the proportion of misbehaving vehicles increases. At the beginning we assume that all participating vehicles are honest, i.e., the proportion of misbehaving vehicles is equivalent to 0, and the PDR can be nearly 70%. In case when all the nodes are misbehaving, the proportion of misbehaving nodes is equivalent to 100%, the PDR falls down to only 20%. If the ratio of misbehaving nodes is 100%, as the misbehaving vehicular node will only forward its self-created messages bundle and refused to deliver those created by other vehicles. In such cases, the PDR can be larger than 0 subsequently every node directly carries its own created message from a source point to the destination point.

The dotted-line curvature in Fig. 2 depicted the decline tendency of the PDR relative to no misbehaving nodes. The graph clearly illustrates the lower percentage of the PDR if more misbehaving nodes exist over the network.

Fig. 3 demonstrates the impact of the misbehaving vehicles on the delay factors and the relative delay of the system. The double-line curve shows the increased tendency of the transmission delay as the proportion of misbehaving nodes increases. Fig. 3 depicted that the transmission delay is in the defined range of 6000 to 7600 s where all the participating vehicles are honest. As the proportion of misbehaving vehicles increases, the transmission delay will rise exponentially.

Transmission delay will rose to 7400 s in worst case scenario where all the participating vehicles are misbehaving. The dashed-line curve depicted the higher proportion of the transmission delay under the different proportions of misbehaving nodes.

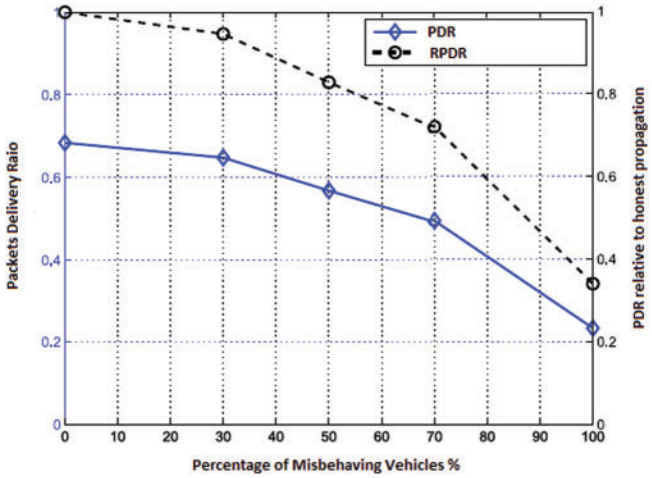

Figure 2: Packet delivery ratio and relative friction for different percentage of misbehaving vehicles

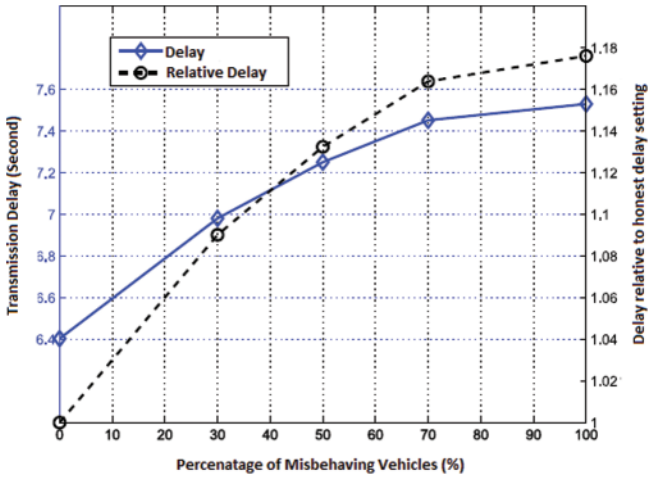

Figure 3: Transmission delay and relative friction under different percentage of misbehaving nodes

As depicted in Figs 2 and 3, the presence of the misbehaving nodes will eventually drop down the packet delivery ratio and increase transmission delay. Thus, message forwarding can be greatly affected by the high proportion of misbehaving nodes, and it is very essential to introduce the reward- based incentive approach to stimulate node contribution in the message forwarding over the network.

We also proposed a unique node identification mechanism scheme by generating a certified public key attached with each message. Public key mechanism is taking into consideration to ensure reliable and accurate message dissemination.

Fig. 4 illustrated the total and average rewarded credits of the suggested scheme with two different scenarios. Total number of created messages also varies from 500 to 1500. At this point, total rewarded incentives refers to the sum of the rewarded incentives of all the forwarded messages, while average rewarded incentives refers to the average rewarded incentives for each forwarded message bundle in the network. The time to live (TTL) per delivered message in Fig. 4 is nearly 600 s. The solid-line curvatures depicted the total rewarded incentives, the curve raises almost exponentially as the number of created messages increases. It is very obvious from Figs. 4 and 5 that increase in the number of generated messages, the aggregated rewarded incentives will be escalated exponentially with the increase ratio of delivered messages at the destination point. In comparison with our proposed incentive driven misbehavior avoidance (IDMA) scheme, the total rewarded credits are much higher than that of the incentive-based misbehavior detection and tolerance (IMDT) scheme. Dotted-line curves depicted the average rewarded incentives for every conveyed message of the proposed incentive-driven forwarding schemes. Moreover, the average rewarded incentives in the proposed IDMA approach are much higher than that of the existing IMDT approach. Figs. 4 and 5 shows that the average rewarded incentives of the proposed incentive-driven scheme are quite stable, as the credits are rewarded from the roadside servers after validation and verification of FwdSig lock-script. This also endorses our previous claims that the rewards imbursement from source nodes for every conveyed message is highly restricted.

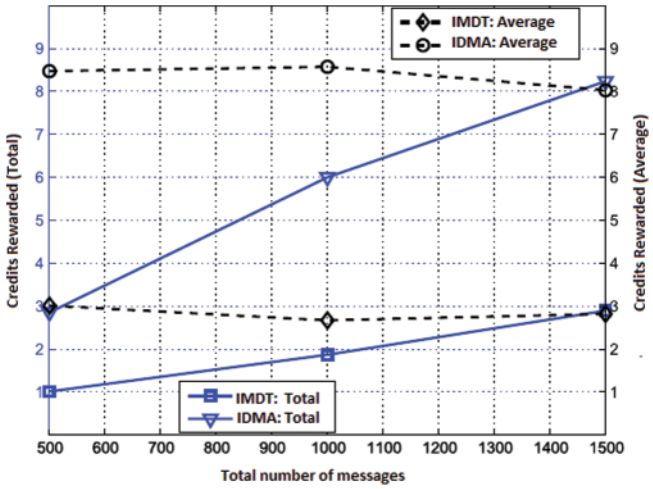

Figure 4: Total rewarded and average rewarded credits for different number of generated messages

The proposed incentive-driven scheme where all the vehicles in the network will have honestly delivered the messages; this clearly shows that the proposed scheme is incentive compatible. For this purpose, the packets can be dealt for brief time at the destination by introducing a buffer. The buffer stores the incoming packets from the source for a given time interval. After elapsing the given time interval these data packets assemble with each other.

Fig. 5 depicted the effects of the TTL of delivered messages, TTL values varies from 2000s to 4000s in the system model. The idea of the total number of rewarded incentives and average rewarded incentives is similar as illustrated in Fig. 4. The rewarded credits in the demonstrated mechanism are depend on the node's cooperation time. TTL is exponentially increased with an increase in the total cooperation time of the participating node in message forwarding process.

As a result, the number of conveyed messages is directly proportional to TTL values. The solid line curve in Fig. 5 illustrates the impacts of the time-to-live ratio on the total rewarded incentives of the proposed scheme. Fig. 5 shows that the total rewarded incentives of the IMDT mechanism is less than that of the IDMA mechanism. The dotted-line curve illustrates the outcome of the time-to-live ratio on the average rewarded incentives per conveyed packet, which demonstrated that the average incentives of the incentive-driven mechanism are exponentially increase with the high TTL value. In the same way, the average rewarded incentives of the IMDT mechanism are much less than that of the IDMA mechanism.

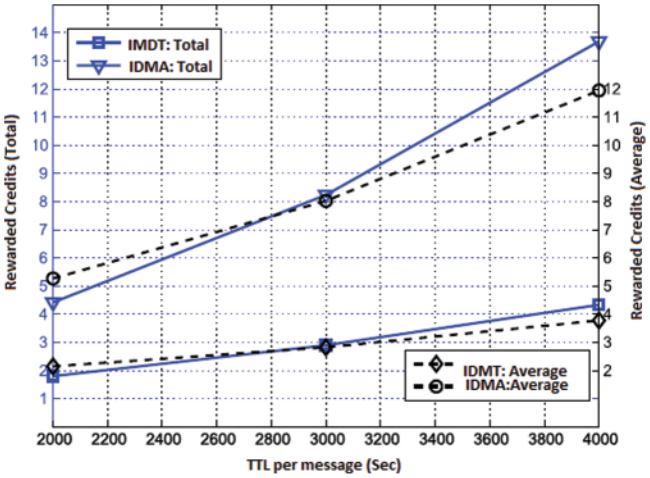

Figure 5: Total rewarded and average rewarded credits under different number of TTL per message

Moreover, we tested the experiment with constant Ω value; Fig. 6 compares the ultimate outcomes about the average reputation with two values of Ω and malicious nodes rate.

All the outcomes about average reputation values were positive; this is due to the fact that the number of vehicles getting feedback in response to sending messages is much higher than the number of vehicles getting feedback in response of generating messages. The outcomes showed that average reputation is impacted by Ω; the four experimental results about average reputation with $\Omega = 1.00$ are higher than for the four tests with $\Omega = 0.5$. This can be clarified on the basis that the weightage given to forward message is high; while the weightage given for the generating messages is low. Because a large number of vehicular nodes receiving negative feedbacks in response to create and flood bogus messages, and fewer nodes receive positive feedbacks for forwarding real and honest data.

Fig. 7 represents the cooperation or participation ratio of the vehicles within the VANET. As discussed earlier in the paper, the participation ratio depends on the incentive-driven model and the number of legitimate vehicles within VANET. The vehicles appear to be cooperative when they get compensated rewards for their support, that's why there is an exponential increment in participation ratio. As depicted within the fig, the vehicular cooperation ratio directly proportional to the number of vehicles in the network. Experimental results show that participation ratio directly influenced by number of vehicles on network.

Fig. 8 depicted the time of creating diverse numbers of certificates for every vehicular node using an elliptic curve cryptographic scheme. The total number of generated certificates comprises two main parameter of digital signature and a pair of cryptographic key combinations. The results show that computational time increases as the number of generated certificates increases. these two-performance metrics are directly proportional to each other. Moreover, resources utilization also increases with the increased number of generated certificates. The line appears in the depicted graph is not plane and an unexpected increase can be observed in computation time when the total number of generated certificates crosses 300. Due to this reason, the maximum limit value is set to 250, due to the reason that not more than 250 certifications will be granted at the same time, so the overhead can be reduced on certificate authority.

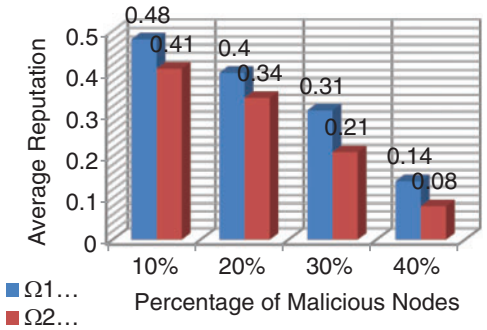

Figure 6: Total rewarded credits and average rewarded credits for different number of messages

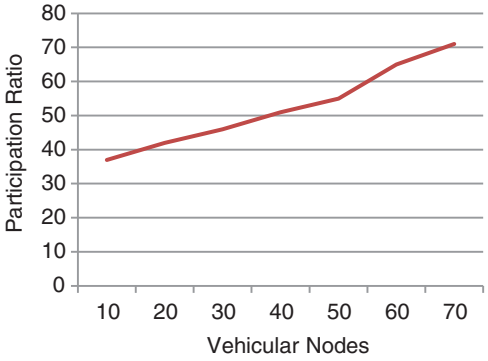

Figure 7: Total rewarded and average rewarded credits for different number of generated messages

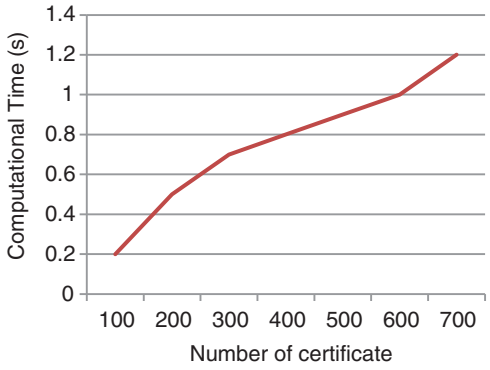

Figure 8: Total rewarded credits and average rewarded credits for different number of messages

5 Conclusion

In this paper, we proposed an incentive-driven scheme incorporating certified public key generation for VANETS. In order to avoid nodes from misbehaving, a stimulus approach is adopted where vehicles can get rewards for their volunteer efforts and positive cooperation with other vehicles on the network. In proposed scheme, fairness and security can be guaranteed by using FwdSig validation and verification mechanism so that a message carrying node can claim the amount of credit only if the node successfully transfers the message bundle to the target point. To realize the objectives of fairness, we also employed 2-of-2 FwdSig lock and unlock scripts incorporated with time-locked condition to deal with fair incentive rewarding. Moreover, in comparison with the existing schemes, our proposed incentive-driven scheme can be deployed reasonably because the proposed scheme does not implement any virtual incentive system on VANETs.

Acknowledgement: Authors acknowledge the financial support of TAIF University researchers supporting project under grant TURSP-2020/21.

Funding Statement: This research was financially supported in part by Researchers Supporting Project (TURSP-2020/121), Taif University, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] V. Maio, R. Brundo and I. Brandic, "Energy and profit aware proof-of-stake offloading in blockchain-based VANETs," in *Proc. UCC 19 12th IEEE/ACM Int. Conf. on Utility and Cloud Computing*, Auckland, New Zealand, pp. 177–186, 2019.

[2] X. Li, J. Liu, X. Li and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in *Proc. 5th Int. Conf. on Intelligent Networking and Collaborative Systems (INCoS)*, Xi'an, IEEE, pp. 210–214, 2013.

[3] F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun, "An overview of internet of vehicles," *China Communication*, vol. 11, no. 10, pp. 1–15, 2014.

[4] Q. Li, A. Malip, K. M. Martin, S.-L. Ng and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Transaction on Vehicular Technology*, vol. 61, no. 9, pp. 4095–4108, 2012.

[5] Z. Cao, Q. Li, H. W. Lim and J. Zhang, "A multi-hop reputation announcement scheme for vanets," in *Proc. IEEE Int. Conf. on Service Operations and Logistics, and Informatics (SOLI)*, China, IEEE, pp. 238–243, 2014.

[6] A. Malip, "Anonymous authenticated announcement schemes in vehicular ad hoc networks," PhD thesis. Information Security Group, Department of Mathematics Royal Holloway, Unive*RSi*ty of London, 2014.

[7] A. Rivero-Garcia, I. Santos-Gonzalez, P. Caballero-Gil and C. Caballero-Gil, "Vanet event verification based on user trust," in *Proc. Parallel, Distributed, and Network Bed Processing (PDP), 24th Euromicro Int. Conf. IEEE*, Heraklion, Crete, Greece, pp. 313–316, 2016.

[8] Z. Ning, "A cooperative quality-aware service access system for social Internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2506–2517, 2018.

[9] D. B. Rawat, B. Bista, G. Yan and M. C. Weigle, "Securing vehicular ad-hoc networks against malicious drivers: A probabilistic approach," in *Proc. IEEE CISIS*, Seoul, South Korea, pp. 146–151, 2011.

[10] L. Chen, Q. Li, K. M. Martin and S.-L. Ng, "Private reputation retrieval in public-a privacy-aware announcement scheme for VANETs," *IET Information Security*, vol. 11, no. 4, pp. 204–210, 2016.

[11] Z. Lu, Q. Wang, G. Qu and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs in Proc," in *17th IEEE Int. Conf. on Trust, Security and privacy in Computing and Communications/12th IEEE Int. Conf. on Big Data Science and Engineering (TrustCom/BigDataSE)*, New York, IEEE, pp. 98–103, 2018.

[12] D. Zhang, F. R. Yu, R. Yang and H. Tang, "A deep reinforcement learning-based trust management scheme for software-defined vehicular networks," in *Proc. 8th ACM Symp. on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet)*, ACM, Montreal, pp. 1–7, 2018.

[13] I. Das Das, R. P. Singh, P. Johri and A. Kumar, *Trust-Based Scheme for Location Finding in Vanets Using Trustworthiness of Node,* New Delhi: Data and Communication Networks, Springer, pp. 43–55, 2019.

[14] A. Kumar, S. Bhardwaj, P. Malik and P. Dabas, "An enhanced reputation-based data forwarding mechanism for VANETs," in *Proc. Int. Conf. on Communications and Cyber Physical Engineering*, Singapore, Springer, pp. 251–259, 2018.

[15] Q. Li, A. Malip, K. M. Martin, S.-L. Ng and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 9, pp. 4095–4108, 2012.

[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 Journal on Wireless Communications and Networking*, vol. 2014, no. 1, pp. 1–13, 2014.

[17] Y. Park, C. Sur and K. H. Rhee, "A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency," *Security and Communication Networks*, vol. 18, no. 3, pp. 1–13, 2018.

[18] R. Sun, Y. Huang and L. Zhu, "Communication by credence credit based: Trust communication in vehicular ad hoc networks," *Mobile Network Application*, vol. 71, pp. 1–13, 2021.

[19] P. Sankar, A. Kumar and B. Bharathi, "Blockchain-based incentive announcement in vanet using creditcoin, advances in electronics," *Communication and Computing*, vol. 709, pp. 567–574, 2021.

[20] I. C. Chang, C.-E. Yen and J. Lo, "An integrated credit-based incentive protocol for symbol-level network-coded cooperative content distribution among vehicular nodes," *Applied Sciences*, vol. 8, no. 11, pp. 1–27, 2018.

[21] L. Alouache, N. Nguyen, M. Aliouat and R. Chelouah, "Credit based incentive approach for V2V cooperation in vehicular cloud computing," *Internet of Vehicles*, vol. 11253, pp. 92–105, 2018.

[22] B. Chen and M. Chan, "MobiCent: A credit-based incentive system for disruption tolerant network," in *Proc. of the IEEE Infocom*, San Diego, CA, USA, pp. 1–9, 2010.

[23] G. Zhao, M. Chen and X. Wei, "RIS: A reciprocal incentive scheme in selfish opportunistic networks," *Wireless Personal. Communication*, vol. 70, no. 4, pp. 1711–1734, 2013.

[24] H. Liu, P. C. Lee and J. C. S. Lui, "On the credit evolution of credit-based incentive protocols in wireless mesh networks," *Computer Network*, vol. 57, no. 17, pp. 3327–3343, 2013.

[25] T. Seregina, O. Brun, R. El-Azouzi and B. J. Prabhu, "On the design of a reward-based incentive mechanism for delay tolerant networks," *IEEE Transaction on Mobile Computing*, vol. 16, no. 2, pp. 453–465, 2017.

[26] H. Jethawa and S. Madria, "Reputation and credit-based incentive mechanism for data-centric message delivery in DTNs," in *Proc. 19th IEEE Int. Conf. on Mobile Data Management (MDM)*, Aalborg, Denmark, pp. 207–216, 2018.

[27] J. Li, X. Wang and R. Yu, "Reputation-based incentives for data dissemination in mobile participatory sensing networks," *International Journal of Distributed Sensor Network*, vol. 11, no. 12, pp. 172130, 2015.

[28] A. Katmada, A. Satsiou and I. Kompatsiaris, "A reputation-based incentive mechanism for a crowd-sourcing platform for financial awareness," in *Proc. of Int. Workshop on the Internet for Financial Collective Awareness and Intelligence*, Florence, Italy, pp. 57–80, 2016.

[29] Y. Zhan, Y. Xia, J. Zhang and Y. Wang, "Incentive mechanism design in mobile opportunistic data collection with time sensitivity," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 246–256, 2018.

[30] I. Chang and J. Lo, "A credit-based incentive protocol for stimulating network-coded cooperative content distribution in VANET," in *Proc. of Eighth Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2014)*, Birmingham, UK, pp. 452–457, 2014.