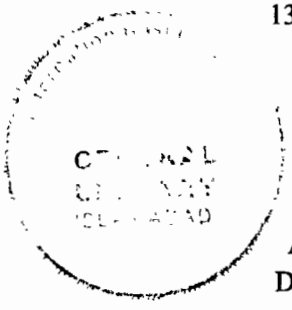
Cooperation Based Misbehavior Avoidance in Vehicular Communication using Stimulus Approach

Ph.D Thesis

By

Shahid Sultan

130-FBAS/PHDCS/F15



Supervised by

Dr. Qaisar Javaid
Assistant Professor
DCS&SE, FBAS, IIUI

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING
FACULTY OF BASIC & APPLIED SCIENCES
INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD PAKISTAN
2022

Vehicular and hoc networks (Comput
computer networks- Security measures
Comput systems (Computer Science)
Fault to
Cyber systems- Security measures

A Dissertation submitted to the

Department of Computer Science and Software Engineering

International Islamic University Islamabad

as a partial fulfillment of requirements for the award of

the degree of

Doctorate of Philosophy in Computer Science

INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD
FACULTY OF BASIC & APPLIED SCIENCES
DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

Date: 20-07-2022

Final Approval

It is certified that we have read this thesis, entitled "Cooperation Based Misbehavior Avoidance in Vehicular Communication using Stimulus Approach" submitted by Mr. Shahid Sultan, Registration No. 130-FBAS/PHDCS/F15. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for the award of the degree of PhD in Computer Science.

Committee

External Examiners:

Prof. Dr. Muazzam Khan,
Quaid-i-Azam University,
Islamabad.

Prof. Dr. Munam Ali Shah,
Comsats University,
Islamabad Campus.

Internal Examiner:

Dr. Muhammad Nadeem,
Assistant professor
Department of Computer Science & Software Engineering
FBAS, IIUI

Supervisor:

Dr. Qaisar Javaid,
Assistant Professor
Department of Computer Science & Software Engineering
FBAS, IIUI

Declaration

I hereby declare that this thesis, neither as a whole nor as a part thereof has been copied out from any source. It is further declared that no portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Shahid Sultan

Dedication

This research is lovingly dedicated to my Parents, Brothers, Sisters, Wife, Anshal Sahar, Syed Muhammad Hassan, and Syed Muhammad Hussain (Sweet Kid).

Shahid Sultan

Acknowledgments

I am deeply grateful to Almighty **ALLAH** for his favors and blessings, which encourage me to write this dissertation. I owe thanks to **ALLAH** for giving me a life full of strength and inspiration to accomplish this task.

This thesis would not have been possible without the inspiration and support of many wonderful individuals, my thanks and appreciation to all of them for being part of this journey and making this thesis possible.

Foremost, I would like to express my sincere gratitude to my supervisor, *Dr. Qaisar Javaid,* for giving me guidance and counsel, and for having faith and confidence in me. It was his invaluable guidance, endless patience, and appreciation that helped me to complete my dissertation in this current shape. I would also like to thank other respected faculty members of the Department of Computer Science and Software Engineering who taught me courses or helped me in some other ways. The administrative staff of the Department of Computer Science and Software Engineering also deserves the recognition of their service throughout my degree.

I am also indebted to my friends both at campus and outside of it whose presence during my PhD made my life rich. The list includes Tabiullah, Sartaj, Fida Hussain, Muhammad Rashid, Abdusalam, and Noor Hamid Mehsud.

This achievement would not have been possible without the pure love and support of my loving family. I appreciate my extended family for their patience, encouragement, and moral support during this long journey. I would not have been able to complete this daunting task.

List of Publication

Publication from Dissertation

1. **S. Sultan**, Q. Javaid, E. Rehman, A. Alahmadi, and N. Ullah, "Incentive-Driven Approach for Misbehavior Avoidance in Vehicular Networks," *CMC-Computers, Materials & Continua,* Vol.70 No.3, pp. 6089–6106, 2021. **(Impact factor 3.77)**

2. **S. Sultan**, Q. Javaid, A.J. Malik, F. Al-Turjman, and M. Attique, "Collaborative-trust approach toward malicious node detection in vehicular ad hoc networks," *Environment, Development and Sustainability*, Vol. 24 No. 6, pp.7532-7550, 2022. **(Impact Factor 3.21)**

ABSTRACT

Selfish node detection in Vehicular Ad-hoc Network (VANET) has always been a research hot-spot. An efficient Misbehavior detection scheme is needed to avoid and reduce the factor of selfishness and maliciousness, especially in the case where the selfish beacons exploit the medium. The objective of this research is to calculate the trust weightage of each vehicle over the network and to reduce the intensity of the selfish vehicular nodes in VANETs.

The proposed mechanism comprises of a data trust module and reputation calculating module, which guarantees honest data communication and reduces the false positive rate of malicious vehicular nodes. The trust module integrates direct and indirect reputation value and derives aggregated trust value in connection with key management strategies.

In the proposed scheme, we employed a fair incentive mechanism for the cooperation-aware vehicular communication system. To deploy a comprehensive credit-based rewarding scheme, the proposed reward-based scheme fully depends on secure and reliable cryptographic procedures.

To validate the effectiveness of the proposed scheme we investigate extensive simulations based on performance parameters of transmission delay, packet delivery ratio, effectiveness of credit rewards over network performance, computation overhead, and participation ratio of honest node behavior. The performance evaluation shows that the proposed scheme delivers more priority messages with high true positive rate and low false positive rate.

Key Words: VANET, Misbehavior, Detection and Avoidance, Collaboration, Credit-Coins, Trust, Reputation Score

Table of Contents

LIST OF FIGURES AND TABLES

List of Acronyms

ACs	Admitted Classes
ACH	Auxiliary Cluster Head
ANN	Artificial Neural Network
AODV	Ad-hoc On Demand Vector
ARQ	Automatic Repeat Request
ATR	Acceptance Threshold Rate
ATV	Aggregated Trust Value
BI	Bayesian Inference
bsk_i	Private key for entity *i*
bpk_i	Public key for entity *i*
BARS	Blockchain base Anonymous Reputation System
C_r	Trust and reputation credibility
C_{pk}	Certified Public Key
CA	Certificate Authority
CBT	Cooperative Based Trust
CH	Cluster Head
CTM	Cell Transmission Model
CISCO	Computer Information System Company
CoCoWa	Collaborative Contact-based Watchdog
CBMA	Collaboration Based Misbehavior Avoidance
CO	Cascading Oversample
CSS	Combined Security Scheme
c	Crypto text
CRN	Congested Road Notification
CID	Contributor Identification
C-FEC	Coded Forward Error Correction
D	Defined constant value
DTM	Distributed Trust Model
DMV	Detection of Malicious Vehicles
DSR	Dynamic Source Routing
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
DST	Dempster-Shafer Theory
DSDV	Destination Sequenced Distance Vector
EWM	Event Warning Message
EAM	Event Assessment System
EST	Evaluation Self Trust
EMS	Evaluation Management System
EC	Event Curve
FPR	False Positive Rate
FHR	Fox Hole Region
FEC	Forward Error Correction

GPS	Global Positional System
IT_x	Incentive Transaction
IDS	Intrusion Detection Scheme
IRS	Incident Reputation System
IDMT	Incentive Driven Misbehavior Detection and Tolerance
ICT	Information and Communication Technologies
IT	Incentive Transaction
k	kernel function for data set 'S'
(K, k)	Key pair for MS
LF	Location Finding
LR	Location Response
LTCA	Long Term Certificate Authority
MANET	Mobile Ad-hoc Network
MAC	Media Access Control
MDS	Misbehavior Detection Scheme
MV	Majority of Voting
MRTS	Metric based RPL Trustworthiness Scheme
MSN	Mobile Social Networking
M	Maximum data transmission rate
m	Minimum data transmission rate
M_p $(\dot{G} \rightarrow X_q)$	$\dot{G}$ *to* X_q Mapping
N	Total number of data packets exchanged in network
N_{dp}	Number of drops data packets
N_{dy}	Represents the total number of delay data packets
N_{cp}	Number of changed packets
N_{nr}	Number misrouted data packets
OBU	On Board Unit
OMD	On-demand Misbehavior Detection
OBUs	On Board Units
PCA	Pseudonym Certificate Authority
PKI	Public Key Infrastructure
PNE	Pro-active Neighbor Exchange
PCN	Post-Crash Notification
PBTS	Positional Behavior Base Trust Scheme
PoV	Proof of Verification
PRC	Path Reservation Center
PPS	Payment and Punishment Scheme
PDR	Packet Delivery Ratio
QoS	Quality of Service
RCA	Root Certificate Authority
RSU	Road Side Unit
RSS	Received Signal Strength
RU	Reputation Update
RREQ	Route Request
RPL	Routing Protocol for Low Power and Lossy Networks

RIS	Reciprocal Incentive Scheme
RRM	Road Reservation Matrix
RT	Reputation Table
R_e	Computed reputation scores for each vehicular node 'V'
r_i	Random number for entity *I*
RID	Recipient Identification
RIPA	Reputation-driven Incentive and Punishment Approach
SM	Service Manager
S	Data set of trained samples
$Sign(C_{pk}, m)$	Signature for message *m*
SVM	Support Vector Machine
SA	Sybil attack
SBTES	Similarity Base Trust Evaluation Scheme
SEE	Security Event Evaluator
SER	Security Event Reporter
SDS	Scammer Detection Scheme
TPR	True Positive Rate
TFT	Tit-for-Tat
T	Generated reports set on 'V'
T_s	Transaction Timestamp
$T_y.in$	Credit input transaction for *y*
$T_y.out$	Credit output transaction for *y*
TC	Threshold Curve
UCoC	Uncertainty Of Event
V	Vehicular node
$Vrf(C_{pk}, \Omega)$	Verification for signature Ω
VSNAS	Vehicle Self-organizing Network Assessment Scheme
VDTN	Vehicular Delay Tolerant Network
V_i	Vehicular entity *i*
VIME	Variation Information Maximizing Exploration
VANET	Vehicular Ad-hoc Network
WAVE	Wireless Access Vehicular Environment
WV	Weighted Votes
x	Vehicular behavior vector feature for node 'x'
y	Vehicular behavior vector feature for node 'y'
Y_i	Derived key for entity *y*
Ω	Value range for output value
αj	Lagrange multiplier for node 'j'
μ	Mean values
$\eth$	Standard deviation

1. Introduction

Vehicular Ad-hoc Network (VANET) is defined as the subcategory of Mobile Ad-hoc Network (MANET); designed for the purpose of communication across vehicles on roads. VANET is an intelligent transportation model that enables vehicles to equip with a set of standards that are necessary for intelligent communication among vehicles.

1.1 Vehicular Ad-hoc Network

The rapid advancement in the field of communication technologies has allowed the use of Ad-hoc network technologies in several different areas. Ad-hoc network technologies are designed for a short period and are autonomous. Vehicular Network is termed one of the prominent counted emerging applications of this field. VANET allows two major types of communication among vehicles, one is intra-vehicular or vehicle to vehicle, and the second one is vehicles to infrastructure or roadside communication. VANET differs from MANET in the characteristic that in mobile ad-hoc network objects or nodes move randomly in its fashion, while in vehicular communication the objects or nodes move in an organized pattern or pre-define pathways. Vehicular networks can also enable communication between nodes in the absence of any pre-defined infrastructure. The interconnecting vehicles are fitted out with the latest wireless network technologies expedients to establish data communication between these interconnected nodes.

We are going to categorize vehicular communication with respect to sharing information on roads and its applicability in different areas. In VANET, the participating vehicles become a wireless connection that is routed through whole network. To create a wide range of vehicular networks the vehicle or nodes connect in 100 to 300 meters to each other. According to the reports of WHO (world health organization), around 1.2 million lives are lost during highway accidents and nearly 50 million persons got injuries in traffic collisions annually. Road incidents are likely to be the third leading cause of death in 2010 [1]. Fire and police are supposed to be the first networks that incorporate this technology to communicate with one another for taking security measures.

Safety of vehicle and driver assistance is counted as the most important category in VANET applications. This category is based on sensing data from participating vehicles. One could receive a brake warning message from his preceding vehicle, collision warning, road condition, maintenance information, weather forecast, traffic jams, and navigational information. Infotainment is another category of information sharing in vehicular networks. Local information sharing is also an important category of VANET applications such as parking space, fuel prices offered at different service stations. It is also helpful in giving information to tourists about sights. Another possible category is car maintenance; one can get online help from his car mechanic in case of car breaks down. In Figure 1.1, a typical VANET-Based real-time data dissemination using Dedicated Short Range Communication (DSRC) is discussed. Mainly three kinds of propagation are discussed in the figure, namely, Vehicle 2 Vehicle, Vehicle 2 Infrastructure and 4/5G, Wi-Max (cellular).

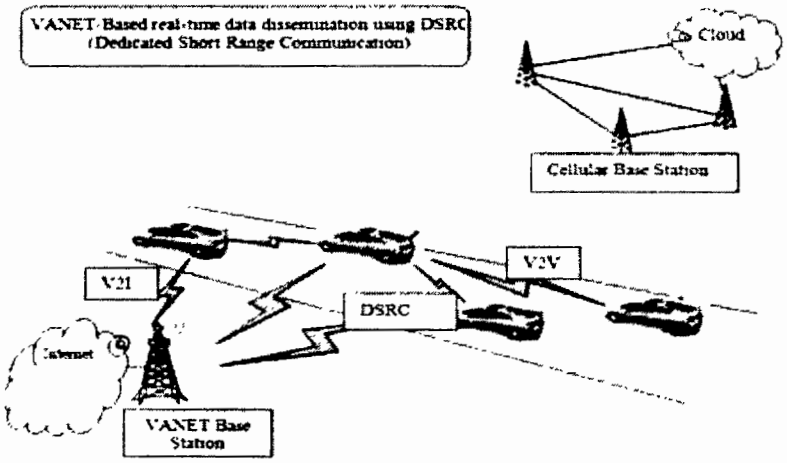


Figure 1.1: VANET Based Real Time Data Dissemination using (DSRC)

Unlike MANET Network, Vehicular Ad-hoc Network has some specific features as follow:

1.1.1 Unbounded Network: Vehicular Ad-hoc Network is unbounded in their nature due to their major implication of large scalability and large-scale movement of vehicles.

1.1.2 Mobility Pattern: VANET adopted its own mobility paradigm and has a pre-defined one-dimensional mobility sequence, but this high mobility of vehicles initiate very short routes that raise challenges for robust propagation of message across the network.

1.1.3 Sparse and Balanced Distribution of Vehicles: In VANET, vehicles are unevenly distributed thus arises the issue of partition and congestion. The partition causes the message to be not easily delivered to the intended receiver.

1.2 Misbehavior in Vehicular Ad-hoc Network

One of the challenging tasks in VANET is the dissemination of robust data and information across the network. The robust data dissemination is a very crucial task to most VANET applications. Thus it requires efficient and robust mobility pattern, speed of the vehicle, number of vehicles, etc. One of the important questions is why misbehavior happens in VANET? In a vehicular ad-hoc network, each vehicle behaves independently. Due to this nature of independence misbehavior occurs. Figure 1.2 illustrates occurrence of misbehavior in VANET. In intentional misbehavior, the attackers disrupt the normal flow of communication in VANET.

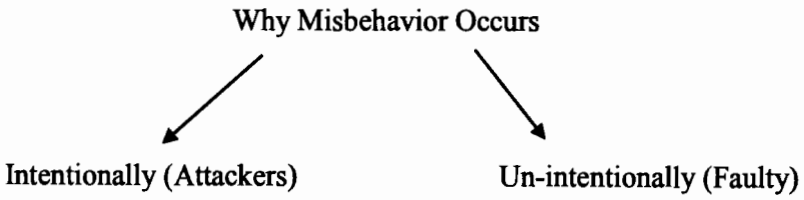


Figure 1.2: Misbehavior Occurrence

1.2.1 Intentional misbehavior

This category of misbehavior comes from the inappropriate intentions of the interacted vehicles to get the inessential settlements by not cooperating with the participating nodes in VANET. Intentional misbehavior includes; Sending bogus alert warnings, discarding/postponement of routing packets, non-cooperation in collective decision making, deny to messages relay, identification spoofing, exchanging of false information in VANET, and so on. Intentional misbehavior is further categorized into two broad

categories; maliciousness and selfishness. Those nodes or vehicles that behave selfishly to save their own resources are called selfishness.

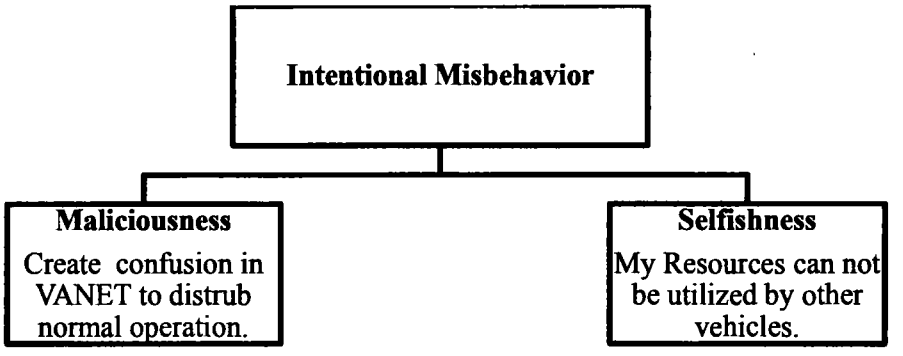


Figure 1.3: Classification of Intentional Misbehavior

While in maliciousness the attackers disturb the normal operation of the network and create confusion in VANET. Selfishness is further categorized into two major types; Node centric selfishness and data-centric selfishness. In the case where vehicle attempt that his resources cannot be utilized by others, this type of selfishness is called node-centric selfishness. While in data-centric selfishness vehicular node propagate false and bogus event-driven messages (congestion) to change the direction and normal flow of traffic.

1.2.2 Un-intentional misbehavior

The category of misbehavior which normally occurs due to motives those are not in the control of contributing users. Participating user/driver of misbehavior node of this category is generally unaware of this undesirable behavior configuration. For example; producing false alerts or event-driven messages due to defective On Board Unit (OBU), fake position information resulting from a malfunction of on-board devices and malevolent behave or by the negotiated nodes are the cases of un-intentional misbehavior nature in VANET.

Two types of communications exchanges in VANET:

Periodic messages: It is usually the status information such as position and speed that exchanges and communicates with other nodes or terminals.

Event-driven: It is a type of broadcast message in case of emergencies such as incidents on roads.

The same control channel is used for both types of message propagation. In VANET the selfish nodes may occupy the whole bandwidth of the channel while the event-generated messages may not propagate on the channel fairly at all and result to compromise the safety in VANET. IEEE 1609 Wireless Access in Vehicular Environment (WAVE) working group has been working on developing standard design in favor of the bottom layer of the protocol heap for VANET, while the 1609 IEEE 802.11p standards describe the MAC layer [2]. The IEEE 802.11p model practices a multi-channel idea and dissimilar admittance classes (ACs) in the direction to row up the extremely appropriate safety communications to guarantee these communications to be able to substitute in a condensed situation [3].

1.3 Motivation and Research Approaches

Although VANET looks rather future success, various future encounters must be considered for achieving effective VANET communication. To further investigate the selfishness we must differentiate the unique features of MANET and VANET.

a. Transmission and communication protocol issues

Different extraordinary velocity communication tools must be projected for VANET. For example, the mobile machinery 2G/2.5G to 4G has gained as long as steadfast safety and widespread communication exposure although 4G is so long as advanced communication volume. But, owing to in elevation latency, inadequate volume and comparatively far above the ground budget, the mobile technologies don't look practicable for VANET. Reduced connectivity and fewer than perfect system presentation may ensue due to meager scattering of vehicles in several geographic areas [4].

b. Dynamic operating atmosphere

VANET has deals with different kinds of operating atmosphere. For instance, the operating environment on road traffic is easy but in case of city environment the communication becomes more complicated due to the hindrances such as buildings, trees or billboards direct communication is usually impossible [5].

c. Improbable VANET simulation system

To endorse the routing protocol stack is appropriate or not, a consistent and precise dynamic prototype must be selected wisely to replicate node moving configurations as close up as factual real road traffic [6].

d. Conduction power restriction

Energy utilization is not an apprehension as the energy power is regularly provided. To attain effectiveness in VANET, the energy needed for trying to find stability particularly in a highly compressed position because it would result in interruption and interference if a high energy power were used.

e. Privacy issues

Privacy is another challenging task in VANET which needs cautious attention when scheming and implementing VANET. Possible threats such as false alert messages shaped by misbehaving nodes could put other vehicular communication and vehicles in danger. The safety design must promise privacy, verification, and veracity to safeguard the linkage from eavesdropping, unlawful data inoculation, and modification [7].

f. Untrustworthy fault recovery technique

The periodic channel in VANET affected by inconsistent message broadcasting puts questions about the consistency of VANET, while some fault retrieval procedures such as ARQ and FEC have been projected. For instance, FEC is inadequate to ensure the consistency in peer-to-peer or unicast approach and henceforth not truly decide the subject. Improving the FEC scheme, another variant called the C-FEC scheme allows exchange among cars when communication is out of the range from access point covering area [8].

g. Network partition subject

Network partitioning is a general problem in VANET when the region of attention is too thin and the number of data-propagating cars is insufficient because signals cannot enter in hindrances such as buildings and trees. How to resolve data dissemination problem in areas that are easy to partition in the network is the most important issue [9].

h. Message inundating problem

Implementing cluster adjacent nodes into practicable units is very crucial because data will propagate ubiquitously and flood the VANET. Improper clustering and boundaries domains can cause vehicles to interfere with radio bandwidth [10].

i. Packet routing problem

Routing in VANET is an intractable problem because of dynamic topology and intermittent links. Routing protocols generally developed for MANET are not appropriate for VANET environments, VANETs use AODV, DSR, and DSDV routing protocols having demonstrated poor message forwarding capabilities with short packet transmission rates. For example, AODV takes lengthier to establish and initiate communication [11].

j. Nodes collaboration issue

Drivers in VANET may apologize to cooperate by progressing information from other vehicles; this selfish behavior degraded the normal flow and performance of the network. Existing detection methods of cooperative nodes, such traditional collaborative approaches could otherwise not be able for resolving the problem because the partner node would deliberately become a self-serving node for communication. In addition to selfishness, misbehavior and malicious nodes are another focus of VANET collaboration. Since the vehicle or node will send fake and deceptive information for malicious reasons, detecting such an error message is more important than identifying a node that is misbehaving. Malicious attackers also send false traffic warnings to other vehicles in VANET, causing drivers to confuse and eventually lead to traffic accidents [12].

Eliminating selfishness is the primary design goal during emergency warning message (EWM) propagation. Due to the absence of identification in the Vehicular Ad-hoc Network, the emergency warning message (EWM) is broadcast out for all the nodes located within a certain area. Therefore, instead of a multi-hop route setup, we adopt a broadcast setup for the dissemination of data.

1.4 Problem Formulation

As misbehavior in vehicular communication is concerned, a lot of different issues and hurdles come in its way. Unlike MANET, we experienced much more critical situation in vehicular communications. We have some specific features that differentiate VANET from

Mobile Ad-hoc Network, like its unbounded nature, large-scale vehicles move in the network area. VANET adopts its own mobility pattern and this feature give rise to the challenge of how to cope with node selfishness. Whereas, in VANET nodes moves at high velocity so it is a critical task to trace the identity of the vehicles. The traditional-based identification approach is not suitable for vehicular networks because the transmission network is sparse and uneven. This feature of VANET causes two issues; one is that of partition of network and the second is congestion of traffic.

When the network is selfish we can compromise emergency messages for the sake of periodic messages. Event-driven messages are more critical as it is primarily associated with safety and security and thus take most of the attention of new researcher that working on messages dissemination in VANET. Both types of event-driven and periodic messages use the same control channels for the propagation of data. When the network is selfish the periodic transmission may occupy the entire bandwidth of the channel as a result of this misbehavior the emergency messages may not be able to propagate on medium at all and resulting to compromise the safety and security of vehicular Ad-hoc Network

Towards selfishness detection in vehicular networks, the following research statements are fine with respect to vehicular communication.

P1: Most of the detection schemes relying on single node information/trust value for misbehavior detection.

Due to lack of collaboration among nodes, most of the existing schemes depend on the reputation from single source of information. The reputation calculation of the existing schemes can be represented in the following Eq. (1.1):

$$R_N(x) = \frac{F_r N(x)}{F_h N(x)} \qquad (1.1)$$

Where, $R_N(x)$ represents the reputation of the node N on the other node x; $F_r N(x)$ represents the total sum of packs received by vehicle x from N for further progressing; $F_h N(x)$ represents the sum of packets received by N and sent by x. The penalty part is responsible for punishing the selfish node. When the reputation assessment of the selfish node x is less than the quantified threshold, the node N probabilistically discards the packs originating

from the node x. vehicular node N not only reduces the reputation value of node x, on the other hand it also informs its neighboring vehicle of the bad behavior of node x, consequently that it might be penalized by all neighbor vehicular nodes.

P2: Difficult to decide whether to cooperate or not with misbehavior node based on calculated node reputation information.

Depends on the calculated trust value, it is very difficult to decide whether to cooperate with the node. The reputation and trust of the node x calculated by the node y is shown in Equation (1.2):

$$R_{xy} = Beta\left(\alpha_{xy}^{new} + 1, \beta_{y}^{new} + 1\right) \quad (1.2)$$

Where, R_{xy} is the reputation value calculated by node x for node y. suppose these nodes have $p + q$ relations, where p and q characterizes positive and false relations respectively. w_{age}Represents the weightiness prearranged to current observation in the choice of {0, 1}. In Eq. (1.3), α_{xy}^{new} characterizes the opportunity that node y has positive repute and calculated by multiply w_{age} with good performance (α_{xy}) of node y and then in addition with positive current interactions among nodes x and y. β_{y}^{new}characterizeoption that node y has corrupt repute and also calculated similarly as signified by Eq. (1.4). Lastly, node x has to take assessment.

$$\alpha_{y}^{new} = (w_{age} \times \alpha_{y}) + p \quad (1.3)$$

$$\beta_{y}^{new} = (w_{age} \times \beta_{y}) + q \quad (1.4)$$

Whether to have a collaboration with node Q or not? The conclusion is represented as B_{pq},as demonstrated in Eq. (1.5), performance of node Pin the direction of node Q and it is a binary rate either 1 (collaborate)or 0 (do not collaborate). The Reputation assessment R_{xy} is provided to decide as follows.

$$B_{xy} = \begin{cases} Cooperate, & T_{xy} \geq B_{xy}, \\ do\ not\ cooperate, & T_{xy} < B_{xy}. \end{cases} \quad (1.5)$$

P3: Determining abnormal nature and streamline a punishment and reward policy for participating nodes.

It is very important to determine that the abnormal behavior rate and the new distrust value of vehicle V can only be calculated by the trustiest or honest verifier in the network.

The parameter T_d is instinctively charted to each vehicle and can be altered when the vehicle is executed as a relay vehicle or as a source vehicle. When the T_d of the vehicular node V alterations, the new T_d is transmitted to the neighbor's vehicles, the neighbors then appraise their whitelist. If the T_d of the vehicle is below the threshold, the vehicle cooperates with the vehicle V. When T_d of the vehicular node V is greater than threshold, its ID must be informed to the relevant CA as a malevolent vehicle. Formerly, the CA announces the ID of the malevolent vehicle V to all participating vehicle and roadside infrastructure. To evaluate value of T_d, CH computes the parameters of vehicle V by equation (6):

$$I_v A = \pi r^2 = \sum_{j=1}^{L} \frac{((1-P_c)^{y_j - x_j}(P_c)^{x_j})}{T_{dj}} \qquad (1.6)$$

Where, L is the sum of verified vehicles participating in network. In equation (1.6), we supposed that vehicle V sends the incoming packets and misses or copying it. The constraint P_c is the probability that a malevolent vehicle loses or copies a packet. The constraints y_j and $x_j$represent the number of packets received by the j^{th} verifier and the number of packets lost or repeated by V, respectively. Shows in Eq. (1.7), CH calculates the standardized usage factor to reduce the impact of a verifier with a high untrusted value. CH uses Eq. (1.6) to calculate the new T_d of V:

$$T_d(new) = T_d(old) + I_v \qquad (1.7)$$

1.4.1 Problem Statement

How to detect node's selfishness in vehicular communication with limited Number of trustiest/ honest verifier while keeping efficient resource provision and customer satisfaction?

1.4.2 Problem Statement Questions

Detection Mechanism Based on Collaboration

How to detect misbehavior and how to determine whether to cooperate with abnormal node or not, relying neighbor node information in VANET communication?

Intentional Non-Forwarding data detection

With limited trustiest or honest verifier, how to identify non-cooperative nodes using reputation model?

Punishment and Reward Policy Based on Behavior Detection

How to optimize punishment and reward policies to stimulate robust data dissemination in VANET?

1.5 Aims and Objectives

One of the extreme primary goals of Vehicular network is to ensure life safety, privacy, and security and ease to the travelers on roads and highways. The main focus of the research is to provide safety exchange of informational data in the shape of messages to the connected vehicles in the network and with the roadside equipment.

Since 2000, the researchers conducting research with automobile manufacturers by the aim to assess the pre-production feasibility to develop effective communication applications. Many engineering prototypes have been developed in order to take into consideration the most critical scenarios, such as emergency event occurring, warning of forward crashes collision avoidance on intersections, lane change warning, stop ahead warning, and vehicle out of control warning.

We can define the research background as in different tracks. In the first track main objective of the research are as under:

- To connect with vehicles in a cooperative network scenario about collision avoidance and safety-related applications.
- To analyze the exchange of information between vehicles and to enable them to identify honest safety and security information and functionalities as the traditional based identification is not suitable for VANET.
- To enhance the performance of the network, and at last initial effective measures.
- The key objective of the second track is the detection of selfishness of nodes. Detection issues will be resolved to ensure that the defined vehicle adheres to safety measures that run across all vehicular devices.
- To develop a trust reputation model is another track of this research; different prototypes and models are developed and maintained.
- To provide designing tools for driver issues track through a framework by which one can measure the real influence of selfishness on the reliability of VANETs. The basic aim of the study is to detect node's selfishness in vehicular communication with limited Number of trustiest/ honest verifier while keeping efficient resource provision and customer satisfaction

- To develop a future prototype that assesses intentional and un-intentional misbehavior. Event driven messages are more critical as it is primarily associated with safety and security and thus take most of the attention of new researcher that working on messages dissemination in VANET
- To identify the misbehavior nodes and how to cope with these policy issues in a largely connected scenario.

Throughout the years, there is an evolution from passive safety systems to active safety systems. Recent research focused on the adoption of state-of-art wireless communication for the next possible steps toward a better vehicular safety system. Such implemented technologies will provide reliable safety in addition to the concurrent support for commercial data transmission. For keeping in account the involvement of both V2V and V2I data communication. Privacy is another challenging task in VANET which needs cautious attention to scheme and implement VANET applications. Possible threats such as false alert messages shaped by misbehaving nodes and could put the other vehicular communication or vehicles in a hazard.

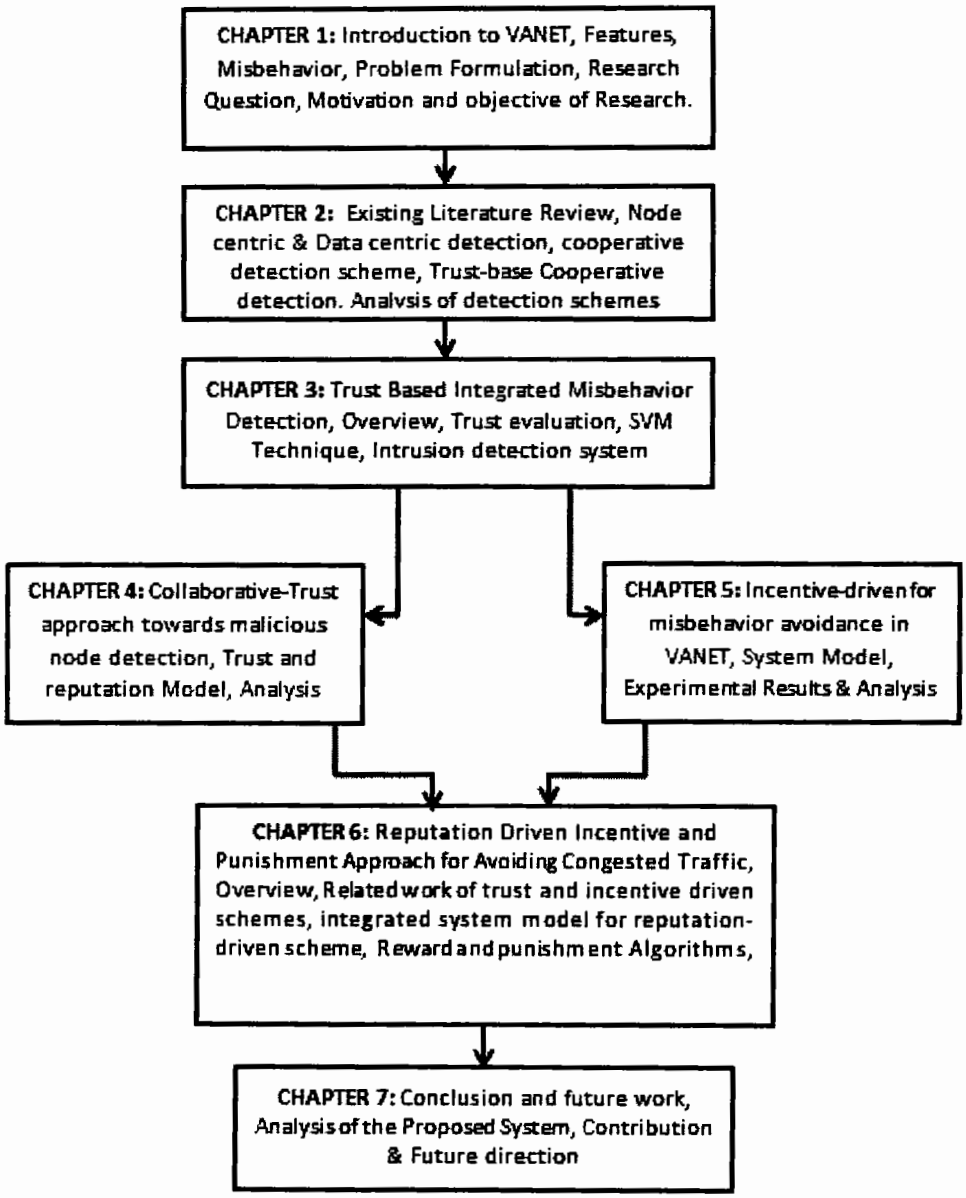


Figure: 1.4: Chapter wise Structure of the Report

2. Literature Review

The effective and reliable data exchange in VANET mainly depends on cooperation of participating nodes, since the existence of a single misbehavior vehicular node can affect communication interruption problems. In this chapter, we explained the existing literature, research methodologies, and their limitations to make a ground for the proposed model. The main purpose of the literature review is to analyze techniques for detecting misbehaving nodes that propagate bogus data packets in VANET. A node that revokes misbehavior is a process that prevents spurious data from participating more in the network. The scheme is divided into two major types, node center, and data center detection. The special emphasis of this literature review is on false information detection schemes in VANET.

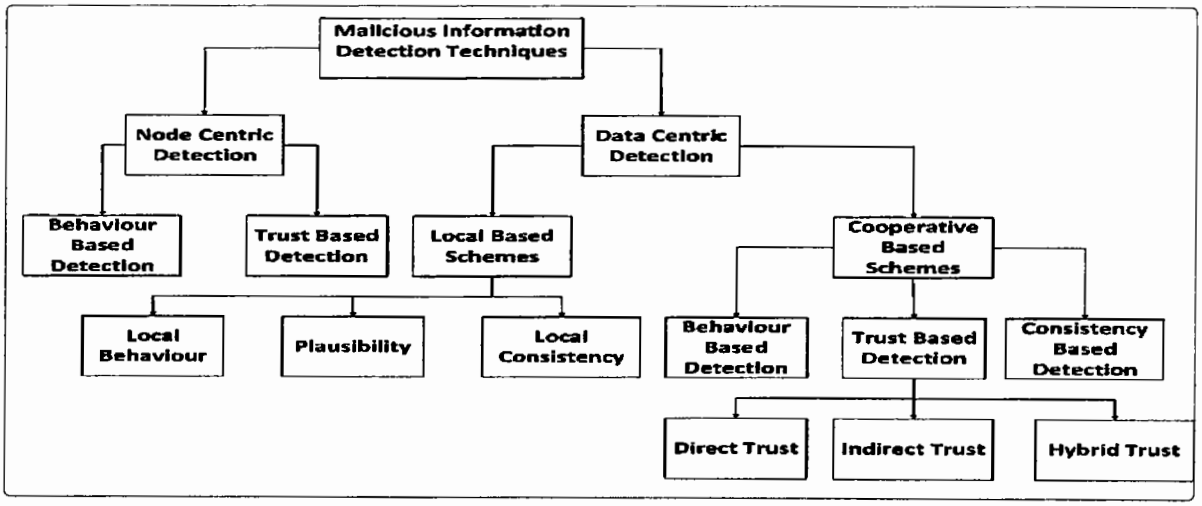


Figure: 2.1: Classification of Detection Schemes in VANET [25]

2.1 Node Centric Detection

The mentioned mechanism mainly involves participating vehicles (nodes) in the vehicle network. This mechanism verifies the bad behavior of a node by analyzing the pattern of packets and messages. Node-centric is further categorized into two comprehensive divisions, behavior-based detection and trust-based detection. Heijden et al [13] suggested

a node-centric detection scheme; the security model screens the node's security identifications, such as digital signatures, with the help of the PKI.

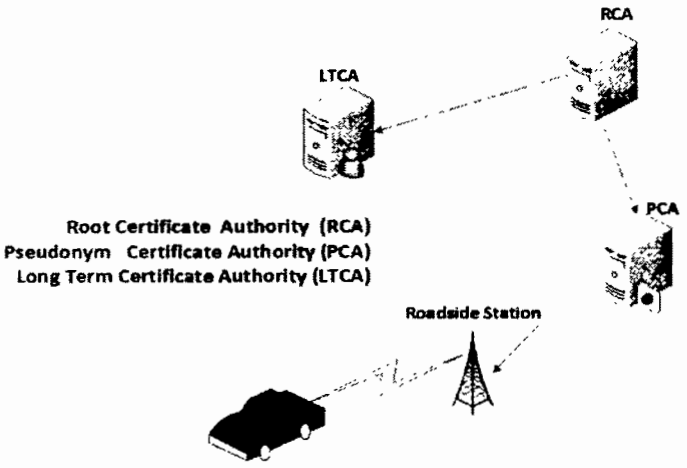


Figure: 2.2: PKI Structure in VANET [25]

2.1.1 Behavior-Based Detection schemes

In these schemes, the normal behavior of participating nodes is monitored in order to recognize how healthy nodes behave. This scheme monitor neighbor node transmission rate and check whether the rate of transmission is exceeding from normal transmission rate [13].

Daeinabi et al. [14] suggested a detection mechanism centered on checking each vehicle in VANET. The proposed scheme implemented detection of malicious vehicles (DMV) algorithm; where a verifier node observes the abnormal behavior (distrust value) of a node. If distrust value increased from a defined threshold the node then reported to the certificate authority (CA). In case, where there is a large number of stakeholders. How to define a reasonable threshold for distrust value? This question is not properly answered in the paper. The authors proposed malicious node detection and prevention mechanism based on mobile agents. Sangulagi et al. [15] demonstrated that software agents can be used to monitor the mobility pattern and power ratio of each vehicle. While a pre-defined threshold is maintained at the source node through this power and mobility comparison is being

made. For evaluation of the effectiveness of the proposed model no routing protocol is employed. Which alternate path can be used if once the malicious route is discovered?

2.1.2 Trust Based Detection Schemes

The scheme depends upon the present and past reputation of an individual node in VANET. A reputation system is maintained for the past communication history of participating vehicular nodes.

Haddadou et al. [16] introduced a new model called VIME, derived from economics signaling theory. This model works in two phases: in the first phase, each participating node has to pay for sending a message to the network, in second phase the cooperating node can be rewarded with an incentive in term of encouragement to communicate honestly. But in the case where the resource is not a constraint for a malicious node to send data into network, this model cannot work efficiently. Haddadou et al. [17] suggested the second model called distributed trust model (DTM^2). In which participating nodes forced to earn credits. In order to decrease malicious data, the cost of sending message should be much higher. Gradually it detects selfish nodes and malicious data but as the density of vehicles increases, this model is insufficient to cope with the situation.

Huang et al. [18] reviewed various trust management mechanisms and concluded that the vibrant environment of vehicular ad-hoc network makes them unfeasible in a practical environment. For the first time, the authors introduced two terminologies of cascading and oversampling of information in VANET. The authors examined that oversampling issues can be arising due to simple voting. A novel voting mechanism is adopted to overcome the limitation of oversampling. Different categories of vehicles have been placed in different voting criteria. The vehicles nearby to the event have much-weighted vote than the others vehicles which are far away from the event that occurred. The author examined the exact time for making decisions in VANET. The work also analyzed that how vehicles make decisions immediately after crash or incident. The suggested work employed a mechanism to wait for other vehicles for getting their suggestions.

2.2 Data Centric Detection Schemes

These schemes analyze the transferred data patterns for any possible misbehavior. The data patterns are associated with other participating vehicles in VANET to confirm duplication of security messages. Khan et al. [19] argued that false safety message transmitted by neighbor vehicle is considered to be a misbehaving node in network. Data-centric detection is further divided into two subcategories. These are local-based and cooperative based detection techniques.

2.2.1 Cooperation Based Detection Schemes

The cooperative data detection scheme analyzes false information node behavior in VANET with the assistance of neighbor vehicular nodes. When a node receives messages, its pattern is cross checked for data redundancy to other participating nodes in the VANET. The neighbor vehicle then confirms the consistency and will guarantee the receiving node to receive the message and acknowledge the sender. The major advantage of this scheme is to recognize misbehavior vehicles in an efficient manner. Cooperative mechanisms will be discus in the literature with details in section 2.3.

2.2.2 Local Based Detection

In this scheme, each piece of safety message is checked independently. The consistency of data is checked from previous and current data transmitted by the participated node. These detection techniques do not depend on other neighbor node's responses. Local-based detection consists of behavior check plausibility check and consistency check mechanisms.

a. Plausibility checking

In the plausibility check model a verification scheme is adopted based on predefined parameters. For example, a single location cannot be occupied by two participating vehicular nodes. Vehicle's speed can be examined through a predefined threshold. Heijden et al. [20] demonstrated that Plausibility prototype can produce effective results in the case where the majority of vehicles are malicious nodes since plausibility examination does not depend on other neighbor evidence.

Consistency calculation has been done with previous and current data transmitted by participating vehicle. These techniques are not dependent on their neighbor vehicle's responses. Dhurandher et al [21] mentioned vehicular security through trust-reputation and plausibility-check approach to address the issue of security in vehicular networks. The proposed algorithm offers security against event-modification attack, fake event-generation, data-aggregation attack, and data-dropping attack. The proposed algorithm not only performs detection but also the isolation of malicious nodes in VANET.

b. Consistency checking

In consistency checking approach the exchanged data is checked from previous and current transmission by a participating node. For example, in the first report node represents location X then in the second report node shows location Y. The velocity from position A to C essentially is consistent in the second scheme. Ruj et al. [22] suggest misbehavior detection scheme to identify error messages and improper behavior of nodes by observing their actions after directing a message. Each node locally determines if the information is accurate or not, this can be done with data-centric approach.

c. Behavior checking

Driver behavior has a key role in detection of misbehavior in VANET. When an event is reported by a vehicle, these schemes monitor the behavior of the reported vehicle.

Hua et al. [23] proposed a comprehensive on-demand misbehavior detection (OMD) technique for location-based routing protocols. The proposed scheme follows three step approaches: location finding (LF), location response (LR), and data progressing. As VANET has a high mobility pattern due to vehicle speed, thus high mobility pattern will directly affect the performance of OMD. Liang et al. [24] provided a very comprehensive overview of the main research perspective and issues in VANET, the architecture of VANET, research methods, recent research issues, challenges in VANET, and discussions on future research trends in VANET. The architecture of VANET is dynamic and changes day by day. New technologies are emerging that needs dynamic security and privacy model.

2.3 Cooperation Based Detection Schemes

Supportive data recognition systems analyses the false information and vehicle behavior in VANET with the assistance of neighboring vehicular nodes. When a node receives data, it is then cross-checked for data redundancy with other participating nodes in the VANET. The neighbor vehicle then confirms the consistency and guarantees that the receiving node accepts the message and acknowledges the participating vehicle's driver. The main advantage of this program is to identify misbehavior efficiently.

Cooperative-based data detection mechanisms can be further categorize into three main classifications i.e. consistency-based, behavior-based, and trust-based detection schemes, as presented in (Fig. 1). The confirmation from neighbor nodes guarantees that the receiving node accepts the message and acknowledges the consistency of the participating node. Thus identification of misbehavior is very efficient in this manner.

Arshad et al. [25] presented a comprehensive overview of malicious and false message dissemination in VANETs. The suggested overview covered the important algorithms for false message detection across VANET. The mentioned research suggested that the classification-based detection mechanism is effective in the case of the congested and condensed networks while a trust-based mechanism showed the best results in the case of high node interaction. The study also suggest that relying on single node information for malicious data detection is not give up to marking and correcting results. The technique only provides good results in high density while its effectiveness decreases with low density.

2.3.1 Cooperative Behavior-Based Detection

To detect false alert information, a comparison model is checked with average driver behavior in VANET. An event is confirmed when the comparison model found similarities in the average behavior of participating vehicles with reporting node behavior. In the case of different behaviors below a defined threshold, a solid foundation will be provided for fake information. These detection schemes depend on large number of honest nodes near the misbehavior node. Molina et al. [26] proposed a detection mechanism that includes error information detection and node isolation in the case of malicious behavior. Non-

cooperative nodes will be isolated from the network if maliciousness is found in the messages. If the vehicle sends false information about traffic jams if "B" is advancing at a smooth speed. Node "B" then reports that "A" is propagating an error alert.

Hernandez et al. [27] presented a cooperative-based approach for the detection of self-centered nodes. A scheme of collaboration is established between local nodes for the awareness of selfishness occurrence. A contact-based watchdog mechanism is adopted where the identity of the node is quickly propagated as soon as misbehavior occurred. This scheme can provide a realistic mechanism to detect selfishness in VANET but at the cost of extra computation overhead and delay.

Chauhua at al. [28] demonstrated the concept of Mobile Social Networking (MSN). The proposed mechanism concluded that the Mobile Social Networking mechanism might replace existing VANET collaboration schemes to arouse cooperation among nodes. MSN scheme has no proper technique to address the issue of latency and packet loss. Social networking-based approach is not adequate when there are limited paths and high mobility of vehicles

2.3.2 Cooperative Consistency-Based Detection

The cooperative consistency based system uses a consistency-check of messages from participating nodes to identify fake information and analyzes the preceding average speed of participating nodes to be essentially consistent with the current speed. If there is a greater difference in the consistency of the calculated speed, this provides reliable evidence of fake information propagation.

Kim et al. [29] distinguished between false alarms and legitimate alarms, security and detection models are implemented in VANET to implement the proposed scheme. The detection model relies on five sources of received information. The driver propagates alert information only after confirming six participating sources. The model relies on these main factors, the threshold curve (TC) and uncertainty of the event (UCoE). The threshold curve (TC) relies on the location of the event and the gap of the drive. The uncertainty of the event curve (UCoE) implies the certainty of the report message from the neighboring

vehicle. If the deterministic of the event curve (CoE) crosses the defined threshold curve, the sender's error alert will be notified. The performance of the system is contingent on these two parameters. The threshold is significant for the driver, and uncertainty of the event is associated with the occurrence of the event. Though, owing to six bases for error or congestion detection, the scheme produces more calculations and delays.

Zaidi et al. [30] analyzed vector routing protocol for monitoring the flooding limits of the network. This work ignored the network performance parameters like bandwidth, delay, and throughput. The proposed scheme only focused on the packet dropped ratio in VANET. Auxiliary information is produced in the results of the main information. Vulimiri et al. [31] demonstrated that auxiliary data is more useful for detecting fake information. The proposed scheme is dependent on how many vehicles produced auxiliary data. Hence it is defined that the relevant information in connection to the main information is called the auxiliary data. The same can be true for the probability that a misbehaving node will also propagate assistance information without primary information. Though, if it is a true primary data, the neighbor vehicle sends some secondary data that generate trust in the primary data domain. In the proposed scheme where the belief level is 1, it represents a real event. A belief level 0 indicates a fake event; however, due to the high mobility, the performance of the scheme will be degraded. Sha et al. [32] proposed role-differentiated (RD4) model for fraudulent data detection using collaborative approach. RD4 filters false positives in VANET. The detection of real accidents is handled by the source of the accident. It is a preliminary solution for detecting malicious data propagated by misbehaving or faulty nodes of VANET. These types of messages built a rule-based relationship between the vehicles as discussed in [33]. At greater densities, pulling out associations between vehicles relying upon a single-vehicle create more computation.

Huang et al. [34] proposed node scammer detection scheme (SDS) for broadcasting false congestion alerts in vehicular network. The proposed mechanism is established on local speed and location that uses radar for verification of congestion events. The proposed scheme uses motion waves for the detection of congested routes and distances. Since the motion wave packet contains a signature and a certificate, it is a very effective anti-

counterfeiting scheme for VANETs. In kinematics, wave packets are used to detect congestion events that do not exist in VANET. This is a very effective way to detect misbehavior for a single vehicle, but as the malicious nodes increases, the detection procedure will receive much time as a result of the distance between the first and the last scammer increasing.

Zaidi et al. [35] suggested a collaborative detection and correction mechanism, where every node computed its flow value (speed, position density, and flow information) and exchange theses information with neighbor nodes. The remaining vehicles also compute values for mentioned parameters. Every node conveys its traffic to the neighbor node. If the received stream does not have pattern matching in the VANET model stream, the data is not accepted. Zaidi eta al. [36] proposed Host-based intrusion detection system (IDS), where vehicular identification used as a statistical model to identify malicious nodes that broadcast fake information. The proposed location verification method fuses its data by regenerating two location verification procedures in a frame called subjective logic. Measurement values have an acceptance threshold rate (ATR) and pro-active neighbor exchange (PNE). Subjective logic expresses the value of truth a combination of beliefs, doubts, and basic interest rates. Heijden et al. [37] stated two kinds of position verification approaches based on minimum Acceptance Threshold Ratio. VANET has a dynamic operating environment and high mobility pattern. Therefore, many parameters can be used in VANET to achieve better results and lower false positive rates.

Harit et al. [38] proposed fox-hole region (FHR) scheme to detect erroneous congested roads and post-crash notifications in VANET. The Misbehave Detection System is based on an FHR occurrence that occurs at a certain point. FHR has a 4-coordinated area whose size depends on the speed of the participating vehicle. Higher FHR means higher speed, and low speed means a smaller FHR. The proposed scheme suggested that the belief value is between D+ and D- for threshold D. These detection methods are suitable for fixed events such as post-crash notifications detection. In some scenarios, the scheme is not feasible where the occurrence is as close as the node may exceed the event position.

Table. 2.1 Cooperation-Based Detection Schemes

Schemes	Detection Type	Technique	Limitations	Privacy	Position	Delay	Overhead	(PF) Rate	Applications
IDS-RC (Intrusion Detection using Revocation Certificates) [40]	Behavior	Comparison of node behavior with that of average behavior using filtering	Degrade performance in case of partitioned network	No	Yes	High	Low	Max	Positional data
RCBD (Root Cause Based Detection) [26]	Behavior	Monitoring of driver behavior with expected range using observer nodes	Dropping of confirmations due to signal loss	No	Yes	High	High	Min	PCN
DBD (Detection Based on Database) [39]	Consistency	Model based data checking and validation mostly used in safety applications	Lack of verification for performance assessment and location privacy	Yes	Yes	High	High	Not mentioned	Not mentioned
DBSSI (Detection Based on Six Source Information) [29]	Consistency	Alert from Six Source confirmation, TC measure Distance between driver and Event while CoE is the valid confirmations.	creation of more positive rate due to minimum threshold definition	No	Yes	High	Low	Min	CRN
SIBD (Secondary Information Based Detection) [31]	Consistency	Used secondary information to detect primary information, implement degree of belief as 1 or 0.	In low density network misbehaved nodes can propagates secondary data	No	No	Low	Low	Min	PCN
RD (Role-differentiated Detection) [32]	Consistency	Signal strength is used as evidence of event from source node, also checks velocity of the neighbor nodes	Degradation in correctness due to high speed	No	No	Low	Low	Min	PCN
VARM (VANET Association Ruling Mining) [33]	Consistency	Text mining of the exchanged messages in comparison with normal routine messages	Calculation of overhead increase even for a solitary vehicle	No	Yes	Low	High	Not mentioned	Not mentioned
CDS (Cheater Detection Scheme) [34]	Consistency	Using radar for velocity and distance checking in case of congested road traffic	Large number of misbehave nodes consumes more time for detection	Yes	Yes	Max	High	Max	CRN
FHR (Fox-Hole Region) [38]	Consistency	Model considered speed of the nodes to obtain degree of belief high speed means high FHR	Only static events considered in this mechanism	Yes	Yes	High	Low	Not mentioned	PCN
C-DAC (Cooperative Detection And Correction) [35]	Consistency	Calculation and exchange of traffic flow values (Speed, Distance, density, location information)	Number of misbehave nodes can degrades system performance	No	Yes	High	High	Not mention	PCN,CRN
Host-IDS(Host Based Intrusion detection System) [36]	Consistency	Used statistical data such as Overhead and FPR, low Overhead and Minimum FPR is to be considered a better approach	A prerequisite mechanism must be followed for honest nodes to detect misbehavior for detection	No	Yes	High	Low	Max	PCN,CRN
SLBD (Subjective Logic Based Detection) [37]	Consistency	Verify position of node using subjective logics (belief, disbelief, uncertainty and base rate)	less number of parameters cannot be used for optimum results	No	Yes	Low	High	Min	Positional data

2.4 Cooperative Trust-Based Detection

Reputation and trust are the key factors to analyze security and provide strong grounds for making decisions in the network. Typically, trust is defined as the degree of confidence and expectation of a participating node to other vehicle activities in the VANET. Trust-based detection techniques allocate standards for vehicles grounded on historical data communications. Trust and reputation model is used to detect and correct malicious data in VANET. This is a generic framework for verifying security information against locally sensing data for Sybil node attack detection. If an inconsistency is found, the data is measured as malicious data. Golle et al. [39] presented a confrontation model based on the parsimony parameters to obtain the best interpretation of correcting data. Having no proper verification or experimental test for this method, it is a very difficult to develop a global database in VANET. Due to lack of providing location privacy, this scheme is not feasible in case where the number of dishonest nodes exceeds the honest node in VANET.

Raya et al. [40] proposed misbehavior eviction scheme, where error location information were tested using bloom filters. The proposed scheme dynamically builds a data model for detecting error information through the comparison of the behavior of each vehicle to the average behavior of other vehicles in its neighborhood. In addition, if a real event occurs at a short density, this will be considered as an error by which is not feasible for security information as demonstrated in [41].

Placzek and Bernas [42] proposed mechanism to detect malicious data in traffic signals at intersections. Nodes generate a large number of wrong identity modules (Sybil attacks), and then pass information from these wrong identities to affect the traffic flow. The proposed scheme used traffic signal model to detect malicious data, it was expected that driver behavior and location verification technology can efficiently detect fake data exchange on intersections. In case of error message from traffic signal, the detection is controlled by the third party control node. The control node provides a trust value to each vehicle for detecting fake data. Falasi et al. [43] proposed detection scheme based on data validation technique; it is assumed that the trust of the node that stops for the green signal is invalid because it will not stop for the go-ahead signal in the selfish condition. Fan and

Wu [44], and Hasrouny et al. [45] investigated different security challenges and proposed a trust based communication model for robust data exchange in VANET. The proposed models suggested comparison criteria that are universally accepted. Soltani and Mizanian [46] investigated limitations of the proposed security model for VANET. The study demonstrated that overhead factor of the network increased as each node retains event information and matching actions to pay attention to selfish nodes. Kim and Bae [47] explained reputation as the level of expectation and self-reliance that a vehicle has on the behavior of another vehicle in VANET.

Ahmed and Kamalrunizam [48] presented overview of the misbehavior detection schemes; most of the existing schemes depend on the present and past reputation of individual node in VANET. A reputation system is maintained for past communication history of participating vehicular nodes. A particular vehicle whose trust score is good in the past communication is expected to behave with honestly in the future. Santos and Moreira [49] presented reputation evaluation scheme in which the nodes received response for the interactive factors of generating and forwarding of packets across VANET. The proposed scheme evaluated the performance of the scheme under different application parameters.

Govindan and Mohapatra [50] investigated a comprehensive review on trust computation and trust dynamics for MANETs. The trust assessment model and misbehavior detection mechanism in MANETs has the potential to preserve network performance while meeting application QoS requirements. Heijdan et al. [51] propose security model which include the constraint for robust privacy, dynamic operating environment, and the temporary nature of connectivity in VANET. The trust-based detection technique assigns nodes values based on their previous data communication history. Lu et al. [52] demonstrated vehicular fog computing to achieve the efficient utilization communication resources in VANET. The proposed mechanism showed better result for greedy forwarding strategies using geographic routing protocol. Ltifi et al. [53] presents a cluster based collaborative trust-management scheme where communicate through a set of messages and follow a dedicated protocol for vehicular communication. The proposed protocol describes the responsibility of every vehicle in the network.

2.4.1 Direct Trust

In direct trust approach the decisions about the trustworthiness of other nodes must be made independently, rather than in contact with other nodes. As a result, trust information from other nodes cannot be gathered in a very short period. Recognized trust is grounded on the joint exchange of information among nodes in VANET. Direct trust does not depend on the trust values of other nodes, and is reasonable for VANET atmosphere.

Text Filtering-Based Detection (TFBD): Text filtering is used in this system to validate the validity of transferred data and to assess the authenticity of surrounding participating vehicle nodes. This approach combines data from several sources of cars into a text filter for each node. Local sensors (digital road map, Radar, lidar, directional antenna) and cooperative awareness message exchange (CAME) between the sender node and neighbor nodes are used to exchange location information.

Bismeyer et al. [54] propose text filtering based detection mechanism, where conversion of two incoming messages is the basis for the proposed scheme. The key benefit of this technique is that it uses neighbor node trust to verify location rather than relying on other cars. The system's correctness is determined by local sensor information, which is influenced by the system's high speed. The disadvantage of this system is the computational overhead and latency of specific vehicle nodes.

Trust-Based Security Scheme for Message Exchange (TSME): The trust-based security scheme for (TSME) uses a grouping catalogue to check for fabricated security event recognition in a vehicular node. Abbasi et al. [55] suggested trust assignment scheme to define a threshold value for each neighboring vehicle in the VANET. The methodology also practices trust to improve decision-making power and uses repeat protocols to check the reply of the reported node. When there is more time between cars to establish connection with the trusted system, this option is practicable.

Positional Behavior-based Trust Scheme (PBTS): Falasi et al. [43] proposed positional behavior based trust scheme to detect malicious-data in traffic signals at highway crossings. Vehicles create multiple fake identities (Sybil attacks) and exchange data from these fake identities to influence traffic signals. To detect malicious data with combined model, driver's expected behavior and location verification technology can be used. If the

information exchange of the traffic lights is wrong, the control system will be monitored by the controlling vehicle. The control node describes the trust threshold of each node to detect malicious information. The modification (update) of the trust value is completed after receiving the information from every vehicular node. Data with low trust value or zero-trust value is regarded as erroneous data. The assumption is not effective for the degree of trust that each node calculates to stop participating in the vehicular communication with the green signal; in the case of selfishness, the particular vehicle will not stay on the green traffic signal light.

2.4.2 Indirect Trust

In the indirect-trust scheme, nodes exchange trust information of other participating nodes based on their past historical communications and relationships. As far as sufficient information is concerned, this trust is transferable and effective.

Proof of Verification (PoV): To detect malicious nodes in VANET, the responsibility for event verification will be borne by the reporting vehicle. Cao et al. [56] demonstrated that when a vehicle senses a security situation, it must be authenticated from participating vehicles in the sensing area and spread to the network. The main disadvantage of this scheme is that misbehaving nodes may use forged digital signatures in the detection area to verify messages. Reporting the low density of VANET in the vehicle area is also known as the disadvantage of this scheme.

Vehicle Ad-hoc Reputation System (VARS): Dotzer et al. [57] proposed Vehicle Ad-hoc reputation system (VARS) to integrate direct and indirect trust values for malicious node detection using decisive conclusions computation on event-driven messages. The main disadvantage of this approach is that it includes collecting reputation evaluations, which is time-consuming.

2.4.3 Hybrid Trust

Hybrid-trust is an arrangement of direct and indirect trust calculations. Hybrid schemes facilitate detection, instead of using direct and indirect trust alone. Author presented a comprehensive survey of important research questions then propose the detection of malicious nodes with highlighted in multi-hop broadcasting in VANET environment.

Incident Reputation System (IRS): The incident reputation system (IRS) avoids incorrect traffic communications in VANET. Lo et al [58] suggested that the vehicular node acquires adequate reputation information from installed sensors and received data. The alert-message will be disseminated to other vehicle nodes in the VANET once sufficient reputation information has been received. The system is based on two factors: the evaluation of event reputation and the evaluation of event confidence. Event table entries of the beacon or event received from the sensor unit mounted on the board. Event ID, event type, event timestamp, event location, event propagation range, event reputation evaluation, and confidence evaluation list are all contained in the event table. The event table keeps track of each occurrence and assigns a reputation rating to it. An event summary monitoring method and a reputation assumption mechanism are used by the IRS. The start of event confidence and the start of event reputation both evaluate the event's intensity and consistency at the same time. The speed of incident reputation evaluation is faster due to the function of the sensor unit (minimum detection), which is IRS's restriction. In a low-density environment, the confidence of the event is low. Other aspects such as incident duration and propagation range also have an impact on IRS.

Event-assessment Model (EAM): Ding et al. [59] proposed an event-based evaluation model in which the event reporting node checks the expected behavior of the event node. If the behaviors match, the evaluation of the event and the evaluation of the reporting node will increase, while the generation of forged information will decrease. Defective or malicious nodes may add incorrect reputation assessments.

Cascading Oversample (CO): Huang et al. [60] demonstrated that due to selfish motives, misbehaving vehicles cannot exchange malicious data in all time intervals. Therefore, depending on the situation in the vehicle network with nodes, honest or misbehaving nodes cannot always be assumed. The shortcomings of trust management are mainly based on election schemes. Another disadvantage of trust management is rollover (when the vehicle node influences other participating nodes during the election process). This phenomenon is called cascaded oversampling and is solved by the following process: In this process, more attention is paid to the vehicle nodes that are very close to the event location than the

vehicle nodes far away from the event location. However, if the distance between the vehicle node and the event is equal, and different opinions are transmitted for the same event, the system will not work properly.

Effective Trust Management System (ETMS): Aniket [61] stated that the issues regarding cascading and oversampling also has a contrary effect on the trust-based management schemes in the VANET. The proposed technique for misbehavior detection follows three mechanisms: misbehavior recognition, Incident rebroadcasting, and overall expulsion and filtrating of fabricated information. Vehicular node maintains incident information and resultant actions to detect misbehaving vehicles. These detection schemes are based on a risk assessment of dishonest vehicle to examine risk intensity and defined threshold. The incident correspondent node sense incidents and generates alert and exchange it with their neighbor's vehicular node. When an observer node observes the behavior of reporter, node outside one step of reporter participates and then forwards the emergency message.

The event reporter's sensed event triggers an alarm, which is broadcast to nearby residents. If the reporter observer in the jump can observe the reporter's behavior, the vehicle that exceeds the reporter's hop point can forward an alert, but the reporter's behavior cannot be detected. There is another well-known factor in falsified information detection, which is delay. Detection schemes with low latency are considered effective and vice versa [62, 63]. VANET is a short-lived network in which the connection time among nodes is of very short-term. VANET is also exposed to various security attacks thus establishing a robust trust-system is a crucial task as investigated in [64-66]. Misbehaving nodes may not always be malicious. The reason depends on multiple conditions in the vehicular networks. A simple trust- based model needs to be implemented for rapid data assessment in VANET. To exchange data over the network a higher trust node and RSU are required by a trust management system for harmful information detection. Due to other responsibilities, RSU has already incurred expenses. Major issue in trust management is the voting system. Because the topology is constantly changing, the threshold cannot be reached. Due to privacy issues, data related to trust has been deleted. For these reasons, VANET may be

needed measurement parameters such as decentralization, scalability, non-safety metrics, acknowledgments, security, privacy, robustness, and False Positive (FP) ratio to establish a comprehensive trust model for VANT [67 - 79].

Decentralization: VANET is a dynamic distributed network. As a result, for trustworthy data communication, a decentralized trust management system is required. The trust model decentralizes trust building by using one-to-one or one-to-many interactions. Some rigorous identity verification on the nodes is required before constructing a distributed trust management system in VANET.

Data scarcity: VANET has a dynamic and distributed network type, and it is almost impossible to interact between the same nodes in the future. Due to the short lifetime of the network, the data received for the first time is very important for building trust.

Network scalability: Scalability is considered an important factor in trust management. The density of nodes is higher, and few nodes interact and send information in the network. The observer needs to quickly determine the incoming information. The trust information can be slightly updated according to the network size. To achieve good trust management, Scalability and trust mechanisms are mutually exclusive. Priority is given to nodes that interact often in successful trust management.

Metric: Different types of measurements are utilized in trust management to establish dynamic trust. Post-crash notification (PCN), congestion, and weather condition beacons are some of the trust management system's signs. In the trust management system assigns a credibility value based on the behavior analysis of neighbor nodes, which is additionally propagated in the network. Priority is given to the event reporter who is relatively close to the event location or close in time.

Confidence: Trust management requires VANET's reliability and confidence to eliminate the event's uncertainty. Nodes reporting the same event are given high trust levels by trust management.

Security: The trust management system requires strong security credentials to authenticate the sender of the security information reported in VANET. Generally, PKI is used to verify the authenticity of reporters in VANET.

Privacy: In VANET, decentralized trust management relies on strong authentication of the vehicle, and the use of a single key will bring security risks to the vehicle owner. As a result, utilizing several keys can help to mitigate network privacy concerns. Many pseudonym change technologies have been developed to implement pseudonym change in VANET to ensure location privacy. Table 2 shows that the majority of trust management solutions do not provide adequate privacy.

Robustness: To detect harmful information, VANET requires a quick response detection method. A new trust management system is required, which must take into account existing settings in various VANET schemes. The alert message should take precedence over the node. The trust management system in the VANET should have the least amount of data (data scarcity), be decentralized and scalable, and have good identity verification.

The proposed trust-aware routing algorithm uses the fog servers to calculate the trust weight of each vehicular node.The trust weight is designed based on the misbehavior features uploaded by each vehicle. We assumed that vehicle information can be obtained, communicated, stored and evaluated from the vehicle via the Internet [80-83].

The misbehavior detection method based on the trust evaluation model in VANET has attracted much attention because of its prospective of maintained network performance and meet QoS assessments investigate in [84-87]. Amongst all the problems of trust assessment technology, "how to achieve accurate trust values" and "how to calculate trust" has always been research hotspots.

Li and Song [84] designed a trust supervision mechanism consisting of data and node reputation to deal with such behaviors in VANET. The individual node trust is calculated based on its function trust and the endorsement trust of neighbor node. Therefore, every node can get local evidence by itself and exchange external trust value to other vehicles. Cheng at al. [85] proposed active trust evaluation, includes direct trust evaluation and in-direct trust evaluation. Evaluation is performed based on the exchange of combined trust-reputation values between two vehicles.

Table 2.2: Trust Based Detection Schemes

MDS	Technique	Decentralized	Scale	Metrics	Assurance	Secure	Privacy	Robust	FP Rate
TFBD (Text Filtering Based Detection) [54]	Text classification of more than one source (Node, Radar, GPS)	+	-	-	+	+	-	-	High
TSME (Trust Based Security For Message Exchange) [55]	Driver behavior and Location verification, Trust management scheme for honest propagation	+	-	+	+	+	-	+	Low
PBTS(Positional Behavior-based Trust Scheme) [43]	Assigned one hop neighbor trust value over the VANET, relative trust calculation done	+	+	+	-	-	-	-	Not Mentioned
VARS (Vehicle Ad-Hoc Reputation System) [57]	Direct and indirect trust calculation integrated with source node verification	+	+	+	+	-	-	-	Not Mentioned
PoV (Proof of Verification) [56]	Reporter node is responsible for event verification with location endorsement	+	+	+	+	+	-	-	Not Mentioned
IRS (Incident Reputation System) [58]	Applied event reputation value and event confidence list	+	+	-	+	+	-	-	Not Mentioned
EAM (Event Assessment Model) [59]	Event observer check the behavior of the reporter driver	+	+	+	+	-	-	-	Low
CO (Cascading Oversample) [60]	Voting mechanism due to dynamic changes	+	-	+	+	+	+	-	High
ETMS (Effective Trust Management System) [61]	Node detection, Event rebroadcast, and Filtering	+	+	-	+	-	+	-	High

Still, most of misbehaving participating vehicular nodes may discard, alter or even exchange fake trust values, while communicating the credibility of other nodes in a non-cooperative environment. To tackle with these limitations, some reputation-based misbehaving nodes detection methods using "vehicular cloud mechanism" have been investigated for VANET. However, it is impractical to use a centralized location to meet the delay requirements.

As far as the incorporation of cloud services and traditional VANET is concerned, cloud mechanism can improve distributed and diverse platforms. As it supports cloud servers and nodes, cloud-enabled VANET can use expanded and efficient computing and memory resources to provide services for moving vehicles [86-88]. Zhang et al. [88] designed a computational offloading method that utilizes the resources of the fog server and vehicle terminal. Soleymani et al. [89] a fuzzy trust model based on historical information and reasonableness was also proposed to secure against different types of threats. In addition, the proposed model selects the cloud node as a tool to evaluate the trust value of VANET. Cloud computing is also a promotion enhancement for mobility provision in the vehicular networks. To select best path for communication in VANET, Noorani and Seno [90] proposed the usage of mobile vehicles, road side units and base stations as cloud servers.

In this part of the thesis, we are moved to propose reputation assessment method that uses collaborative approach to measure the impact of abnormally behaving vehicles on network performance. Employing cloud computing, historical vehicular information can be presented to store and calculate the reputation weightage of each anticipated vehicle. In addition, the cloud we showed enables VANET to deploy cloud server and nodes to track surrounding vehicular nodes and retain their abnormal behavior changes. Therefore, cloud-computing has expediency and functions for active misbehavior monitoring and reputation assessments in VANET.

Owing to the influence of misbehavior on data packets delivery, many trust evaluation methods for dealing with node misbehavior has been considered. Dahmane et al. [91] proposed a trust-aware communication model for VANET to evaluate the trust value based on four parameters reflecting the state of the vehicle. Hu et al. [92] developed a trust-aware recommendation approach that gathers feedback from vehicular nodes to calculate trust

scores. Though, some of them reflect the uncertainty of abnormal behavior factors in VANET. The research work in [93, 94] has shown that misbehaving vehicular nodes adopt active attack approach to reduce the proportion of being identified as malicious in wireless network.

Wu et al. [94] investigated active attacks and malicious attacks with actively changing functions and variable characteristics. Liang et al. [95] proposed a behavior-driven intrusion detection technology to deal with arbitrary and hidden attacker. The pattern and mobility of misbehavior generally result in the inconsistency of service performance. A woven multi-path routing was proposed to ensure the reliability of data packet propagation and meet the end to end delay constraints in WSN To describe the probability and active impact of misbehavior, the proposed work collects parameters to identify the trustworthy value of each vehicle, and calculate the degree of trustworthiness based on the statistical results of the trustworthy state over time. This hypothesis can solve constant misbehavior and random misbehavior. Existing work divides trust modeling in the context of VANET into main categories, namely data-centric trust, node-identity based models and hybrid model. The method of using data-based models to evaluate the reliability of vehicles based on information. The data-based trust model uses several decision logics to evaluate data reports to infer its validity. Wen et al. [96] proposed a data-centric trust calculation algorithm to calculate the credibility of a vehicle from multiple aspects, namely the type of nodes, remaining gasoline, speed and number of vehicle accidents. In this way, it can detect untrusted reputation report or event from all the evidences. A major drawback of this approach is that if a node seeks cooperation from neighbor to deliver and exchange content, data-centric model will fail because they cannot create a trust-relationship between other nodes. The identity-based model divides the media into trust and distrust, and forwards data packets through the media that has established a priori trust relationship. Zhang et al. [97] proposed a consistent ant colony optimization approach with enhanced security awareness, which identifies malicious vehicles and prevents them from participating in communication.

Some trusted vehicles may initiate misbehaviors under switch attack or active attack scenario. Vegni and Little [98] presented that the hybrid trust method can use both the

data-centric model and the node-identity based model, and they can update the trust metric based on the characteristics of each vehicle and the reputation report from the trusted vehicle. However, the mentioned approach does not focus on implementing dynamic evidence about bad behavior to service delivery in a confrontational environment. In this research work, we adopt a hybrid-trust model, and evaluate the trust level of the vehicle by considering the features of each node and the RSS reports of the neighboring nodes at the same time, using timely dynamic information of bad behavior. Therefore, our method can not only defend fixed misbehavior, but also investigate mobile attack and uncertain misbehavior.

Multi-path routing proposed to enhance network performance by accumulative possibility of transmitted data on many paths. Many multi-path routing protocols have been investigated in the related work in [99-102]. Han and Chung [101] combines the features of similarity traffic into a multi-path routing approach that can reduce transmission delay and data packets loss ratio. However, these works study a special kind of selfish behavior in data packet transmission.

Challal et al. [102] proposed a fault-tolerant multi-path routing scheme to improve the reliability of the network under the attack of intruders. In addition to this behavior that directly disrupts transmission; improperly-behaved vehicles will also transmit false location information to nearby vehicles, leading to misleading driving directions or bandwidth consumption. To defend against various bad behaviors, not only the faulty vehicles behavior should be originate, but also definite misbehavior attacks should be noticed. Research work presented in [104-106] suggests multipath routing in networks with faulty node behaviors and malicious attacks to tolerate bad behaviors in the network. Generally, consistency metrics are combined with other existing routing approaches for next-hop and free path selection in VANET. However, the above mentioned multi-path mechanism will ignore the abnormal behavior information under accidental attack or mobile attack. In this research work, we used the dynamic parameters of misbehavior as a performance metric to the design of multi-path routing protocols. Due to intrusion and congestion, wireless network usually have losses in packet transmission. Saad et al. [107]

proposed rate allocation approach and investigated by taking into account the lessee characteristics of the wireless link.

Wing et al. [109] proposed noise perception resource utilization scheme to perform reliable data transmission based on noise metrics in the presence of artificial noise. To maximize the network performance, Saad eta al. [107] and Wing et al. [109] uses QoS requirements as constraints for allocating data channels. On the other side, due to the different levels of loss among users, the fairness between users will be undermined. In this work, we incorporate the trust metric into the impartial functions and restraint condition of the resource utilization problem, and then dynamically regulate a fair flow distribution based on the real loss in data packet transmission.

Wang et al. [108] suggested the distribution of data-traffic between different service areas. The proposed work extended the utility function in the network utilization mechanism issues, namely NUM, to apply to flexible and inelastic data-traffic. Jin et al. [110] merged the theoretical context with the restraint situation of wireless sensor network. The proposed scheme used a utility based traffic distribution approach, which is approachable to various types of network factors. In addition, because of being misbehavior node, proposed scheme used trust-reputation weights in VANET.

To detect false alert information, a comparison model is checked with average driver behavior in VANET. The research work in [111-121] investigated traffic flow models to characterize traffic based on driver behavior and traffic stimuli. Accurate traffic characterization is needed to effectively utilize the VANET infrastructure. An event is confirmed when comparison model found similarities in average behavior of participating vehicle with reporting node behavior. Rehman et al. [122] proposed game-theory reward based mechanism that can be helpful to address selfish behavior using watch-dog approach and to motivate for collaborative participation. Various kinds of cards are allocated to nodes as per their selfish level in the existing approaches. In the proposed scheme, a reputation value is assigned to each node. Malicious node can be identifying using local detection approach (where vehicle detection mechanism cannot be affected by external factors) or cooperative detection approach (where detection mechanism relies on cooperation between vehicles/road side units. Hassan et al [123] demonstrated that

vehicular nodes don't really confide in one another, they may present malicious data in the network and disturb the normal flow by launching denial of service (DoS) attacks. De eta al. [124] suggested a centralized approach which can be used to deal with issues like network scalability, credibility of information, and delay caused by higher network density. Velayudhan et al. [125] investigated that the attacker creates multiple identities that may have associated with a legal and honest node and exchanges information with other legal nodes. In the case of different behaviors below a defined threshold, a solid foundation will be provided for fake information. These detection schemes rely on the largest honest node near the misbehavior node. The mechanism includes error information detection and node isolation in the case of malicious behavior. Non-cooperative nodes will be isolated from network if maliciousness is found in the messages. If the vehicle sends false information about traffic jams, if "B" is advancing at smooth speed. Node "B" then reports that "A" is propagating an error alert.

Zouinkhi et al [126] presented a cooperative based approach for the detection of self-centered nodes. A scheme of collaboration is establish between local nodes for the awareness of selfishness occurrence. A contact based watchdog mechanism is adopted where the identity of node is quickly propagated as soon as misbehavior occurred. This scheme is able to provide a realistic mechanism to detect selfishness in VANET, but at the cost of extra computational overhead and delay. In Collaborative detection and correction, every node computed its own flow value (speed, position density and flow information) then exchanges the information with neighbor nodes. The remaining vehicles also computed values for mentioned parameters. Every node conveys its traffic to neighbor node. If the received stream does not having pattern matching in VANET model stream, the data is not accepted. Heijdan et al. [127] proposed location verification method using subjective logic. Measurement values have an acceptance threshold rate (ATR) and pro-active neighbor exchange (PNE). Subjective logic expresses the value of truth a combination to beliefs, doubts and basic interest rates. Therefore, more parameters can be used in VANET to achieve better results and lower false positive rates.

One of the challenging tasks is how to sense malicious packets in traffic signal at junctions. A vehicle creates multiple fake identities and exchanges data from these IDs to

handle traffic flow in VANET. In order to detect malicious data across the network a combined approach of driver's expected behavior and location verification technology are used. In case of wrong information exchange, control is monitored by neighboring vehicles. The control node describes a trust threshold for each node to detect malicious information. Rrecaj et al. [128] suggested cell transmission model (CTM) to differentiate light, medium and congested traffic situations. Trust value modification is done after receiving trust evaluation reports from each participating node. Evaluation reports having less than the defined threshold value is to be considered as maliciousness. These assumptions are not effective for every network. For example, to stop a participating vehicle on green signal; in case of selfishness situation a vehicle will not stop over green traffic signal. The comparative analysis of the define metrics for different schemes are shown in Table 2.3. Moreover, some detection mechanisms also used network flow difference to observe fake data over the network. Network flow difference does not give up-to mark results because correctness of the data cannot be observed by abnormal traffic data flow. In this section of thesis, we focused on light weight methods to detect malicious node and data over the network.

Table 2.3 Cooperative-Trust Based Detection Schemes

Related work	Detection ratio ≥ 80%	Privacy	Delay	Detection of false injection data	Detection in dynamic networks	Malicious node evolution from honest nodes
Rehman et al. [122]	-	+	-	+	+	+
Hassan et al. [123]	-	+	-	+	+	-
De et al. [124]	+	+	-	-	-	+
Velayudhan et al. [125]	+	-	-	+	-	+
Zouinkhi et al. [126]	+	-	-	+	+	-
Heijdan et al. [127]	-	-	+	-	-	+
Rrecaj eta al. [128]	+	-	+	-	+	-

2.5 Chapter Summary and Analysis

In this chapter, we examined different existing mechanisms in cooperative data detection approaches. The main focus of our research study based on neighbor node-based detection and trust-base detection schemes. Cooperative-based detection schemes are proficient on account of dense VANET scenario with high ratio of cooperative nodes. Trust-aware detection schemes showed great execution when the recurrence of collaboration among vehicles was high. Still, trust-aware scheme and cooperative-based misbehavior node detection has its own challenges and limitations. The existing misbehavior node detection schemes cannot offer reasonable and robust performance due high delay and low density in VANET. As shown in the literature review that most of the schemes are affected with computational overhead and latency constrains. Therefore, VANET need robust detection mechanism that should provide data-scarcity and have least delay in communication.

3. Research Methodology

An effective trust evaluation model can deliver useful information to recognize whether a node is reliable for the exchanging of data over the network. The chapter outlines the detailed framework based on collaborative-trust approach for avoiding misbehavior across the network. We first defined a comprehensive misbehavior detection and avoidance framework based on reputation-trust assessment. The methodology of trust assessment is proposed to evaluate the trust weight of each vehicle. Then, we demonstrate the incorporation of misbehavior detection and avoidance schemes comprised of trust-aware routing and traffic distribution algorithms among multiple entities.

In the route selection and maintenance process, the source discovers or redirects multiple paths to the target node based on the trust record of the middle-ware node. The trust values of different paths should be combined into the traffic distribution algorithm of each source node. As shown in Figure 3.1, the framework process is as follows:

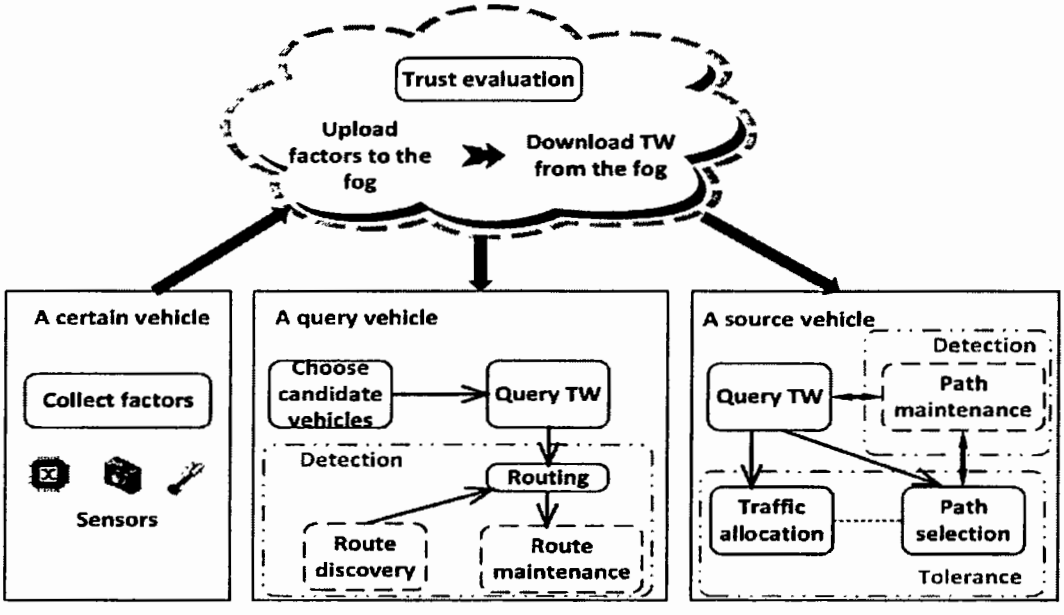


Figure: 3.1: Integrated misbehavior detection in VANET [81]

The main focus of this work is the application of selfish behavior detection technology, provided that the method has a small packet loss rate and reliable terminal throughput. In the proposed scheme, to identify selfish behavior in VANET, it is recommended that each node or vehicle cooperate to forward the data packet to the next neighbor node in the scheme.

Reputation and threshold mechanisms are the main processes and techniques to keep the network load below the defined capacity of the network. If each vehicle node participates in the calculation of reputation and forwards data packets fairly, this scheme is applicable. But this is also related to certain issues, such as media contention, packet conflicts, and message redundancy or duplication.

The current version of the Ad-hoc on-demand vector control protocol uses vehicle status and traditional flooding algorithms to route data packets. The main disadvantage of the flooding algorithm may be the duplication of data packets in the entire system. The Ad-hoc on-demand vector routing protocol uses link information and node status information that cannot provide reliable message distribution for a long conversation.

3.1 Trust and Reputation Calculating Model

The trust calculation phase of the proposed model encourages nodes those acting in a good way and restrict the nodes while acting in a bad way. The detection models based on trust evaluation mechanism in VANET attract much attention due to its prospective for maintaining the network stability and satisfying the QoS applications specifications. The hot topics among the issues related to trust evaluation are, "in order to evaluate trust value for participating vehicular node" and "how to evaluate the credibility of a specific vehicle". VANET is a temporary sort of network where the node connectivity remains for a short span of time and vehicles interact just for few seconds. Trust evaluation for other vehicles must be conducted on individual sites rather than other neighboring vehicular nodes. 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 node on the basis of their past communication information.

A reputation-based detection mechanism scheme that takes confidentiality consideration for VANET is proposed in this section. Here, the vehicular nodes rather than the centralized reputation servers took the decisions to recognize whether a particular vehicular node is honest or not, since every vehicle deemed reputable by its neighbors participating vehicles is given reputation scores, and the average score reveals whether the vehicle is honest or not. In the proposed method we provided a full description of VANET primitives, which allows the proposed mechanism to address a robust mechanism for the repossession of updated reputation scores for each vehicle. We examined that oversampling issues can be arising due to simple voting. A novel voting mechanism is adopted to overcome the limitation of oversampling. Different categories of vehicles have been placed in different voting criteria. The vehicles nearby to the event have much-weighted vote than the others vehicles which are far away from the event occurred. This work also presents analysis and experimentation to calculate the percentage of malicious nodes and their impact in different scenarios.

Misbehavior detection based on the collaborative-trust approach is comprised of the following steps:

Step 1) A direct trust management approach is followed in 1st step where vehicular node 'A' collects communication history table and useful information through the direct communication with Node 'B'.

Step 2) Indirect trust management approach is used in the 2nd step where a vehicular node 'A' requests its neighbor nodes for getting the trust and reputation information of Node 'B'.

Step 3) In the3rd step the indirect trust management approach is followed where node 'A' requests the Road Side Units (RSUs) within its communication range of Node 'A' to access the trust reputation values about Node 'B'.

The direct reputation for a participating vehicle 'B' can be calculated based on collected information from checking the history table for past communication. While indirect reputation can be computed on collected information from neighboring vehicles and road

side units (RSUs). The final calculated reputation value of vehicular node 'B' is based on the direct and indirect reputation computed by vehicular node 'A'. If a node behaves honestly, the calculated reputation value will be high. The model will also calculate the present and past reputation of every individual vehicular node in VANET. This reputation system is preserved for past communication account of participating vehicular nodes. Figure 3.2 depicted the trust calculation of the proposed research work.

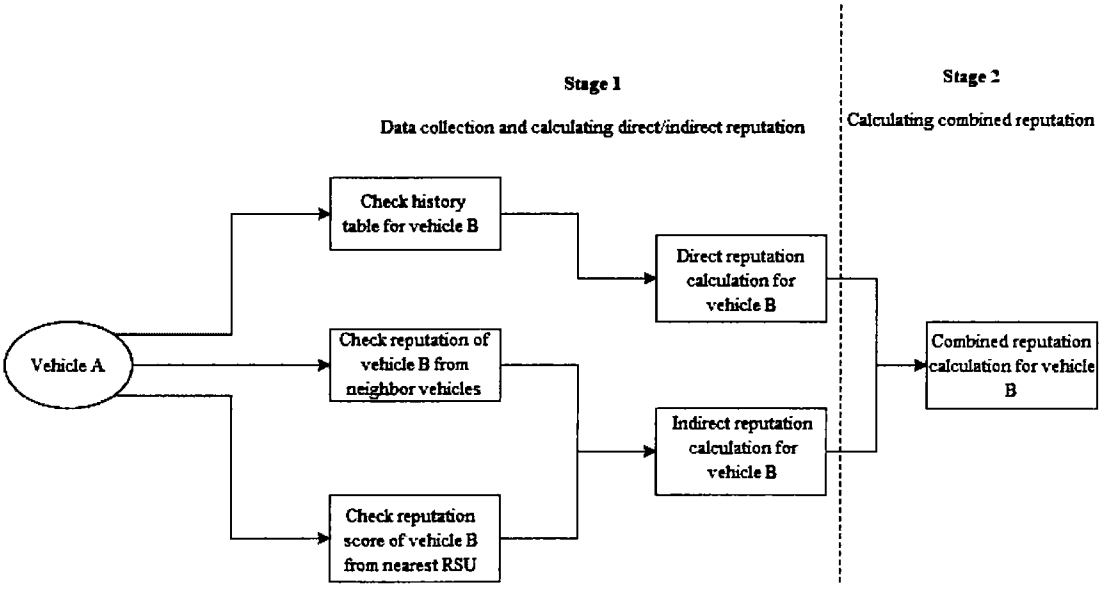


Figure: 3.2: Trust and Reputation Calculating Model

The non-forwarding ratio of node 'B' can be correctly defined by the reputation parameters calculated in the model. For example, a vehicular node 'A' detects that how many data frames exchanged through a defined link (*A*; *B*), and how much accurate data packets went through the malicious recognition process. In this case the reputation value of *r* for a defined link (*A*; *B*) can be computed by Vehicle 'A' by obtaining the actual rate of valid data packets. For example, if vehicular node 'A' wants to compute the reputation of a corresponding receiver node 'B' over a communication link (*A*; *B*), then the calculated value for *r* is defined by the following equation

$$r_{A,B} = Pf_{A,B} / Pf_{A,B} + Pd_{A,B} \qquad (3.1)$$

where r used to represent is the reputation value for vehicular node 'B' that can be directly observed by vehicle 'A', Pf and Pd are the data frames forwarded and the number of frames drops respectively. Let $N(B)$ represents total number forwarding nodes for a specific vehicular node 'B', the reputation value for 'B' can be computed as:

$$r_b = 1/n \sum_{j \in N(B)} rj, B \qquad (3.2)$$

Here, r is the reputation of vehicle B that is directly observed by vehicle A, Pf is the number of data packets forwarded, and Pd is the number of packets discarded or disrupted by Vehicle B. Fog calculates the reputation parameter of the receiver node B. Let $N(B)$ denote as the set of Vehicle B's transmitter nodes, the reputation of Vehicle B can be computed as follows:

Table. 3.1 Parameter factors for ten vehicles [81]

	f1	*f2*	*f3*	*f4*	*f5*	*f6*
v1	0.804	0.94	1	2	2	0.079
v2	0.826	0.95	0.5	1	2	0.081
v3	0.816	0.91	1	0.5	2	0.71
v4	0.251	0.88	2	0.2	1	0.85
v5	0.039	0.91	1	0.5	0.5	0.099
v6	0.702	0.75	0.5	0.3	0.3	0.083
v7	0.604	0.47	0.1	0.5	0.1	0.078
v8	0.715	0.70	0.5	0.3	0.3	0.073
v9	0.764	0.83	0.3	0.3	0.5	0.086
v10	0.853	0.72	0.1	0.2	0.3	0.087

We take an example to describe our trust value evaluation process. There are ten vehicles $v_1; v_2; : : : ; v_{10}$ and six factors $f_1; f_2; : : : ; f_6$ mentioned above, as shown in Table 3.1. the proposed technique of consistency checking using SVM based classification takes linear and no-linear transformation parameters. In the proposed mechanism we used the existing eigen values for linear transformation. The six eigenvalues of principle components are depicted in Fig. 3.3.

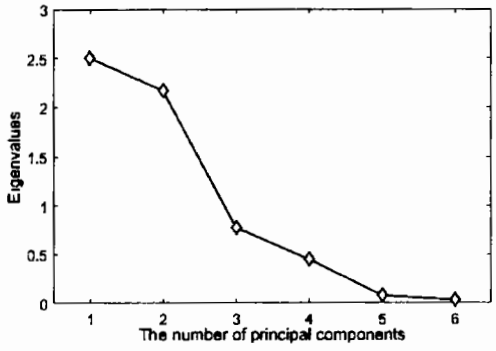


Figure: 3.3: Principal components for eigenvalues [81]

We can see that the first three main factors can replace all components. The trust-value of every vehicle can be acquired in section 3.4. The trust-value of v_4, v_5 and v_7 are smaller than 0.61. The trust-values of define RSS pattern v_4, v_5 are near to 0.5 so that there are maximum two vehicles having similar pattern like ei / ($\sum_{j=1}^{6} ej$) = 0.09973.

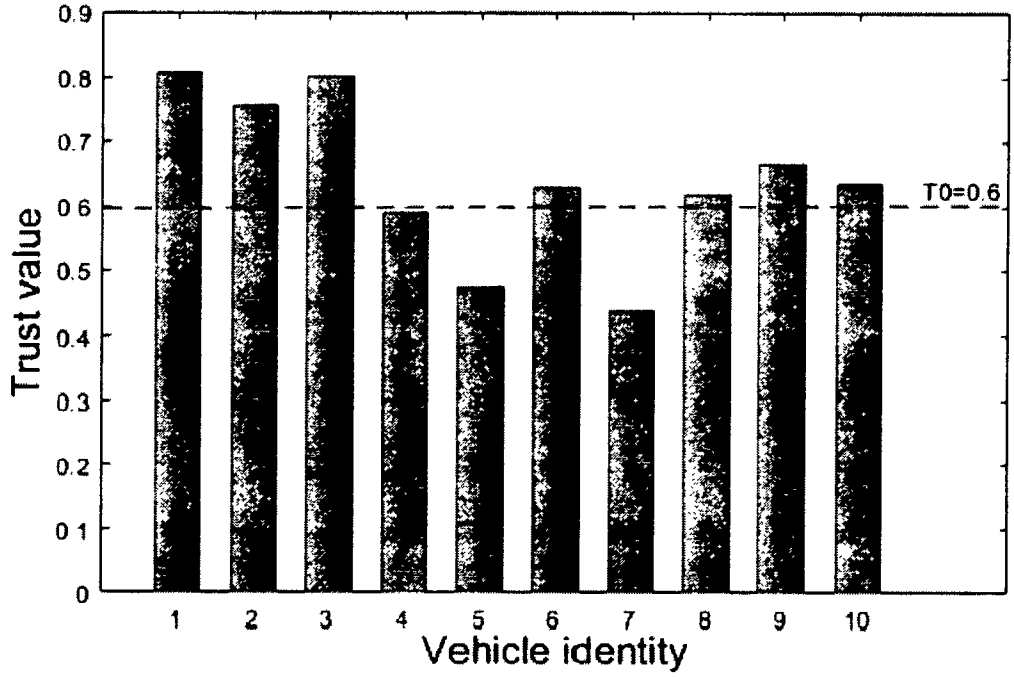


Figure: 3.4: Trust values calculation of each vehicle [81]

We can infer that v_4, v_5 are very similar to be sybil attack. In the meantime, v_7 with f_2 = 0.48 launches packet drop attack, results in a quite lower trust-value after the trust evaluation. Hence, our collaborative trust-evaluation mechanism detected various misbehaviors of nodes very effectively.

3.2 Reputation Update

The CBMA updates three reputations shown as below:

1. When a node initialize a Forward Reputation Score, it increments Forward Reputation Count by 1.

2. When a non-target node accepts a fresh (never seen) packet, it increments it's Frep_Count by 1.

3. When the node forwards the data packet, it increases FP_Count by 1.

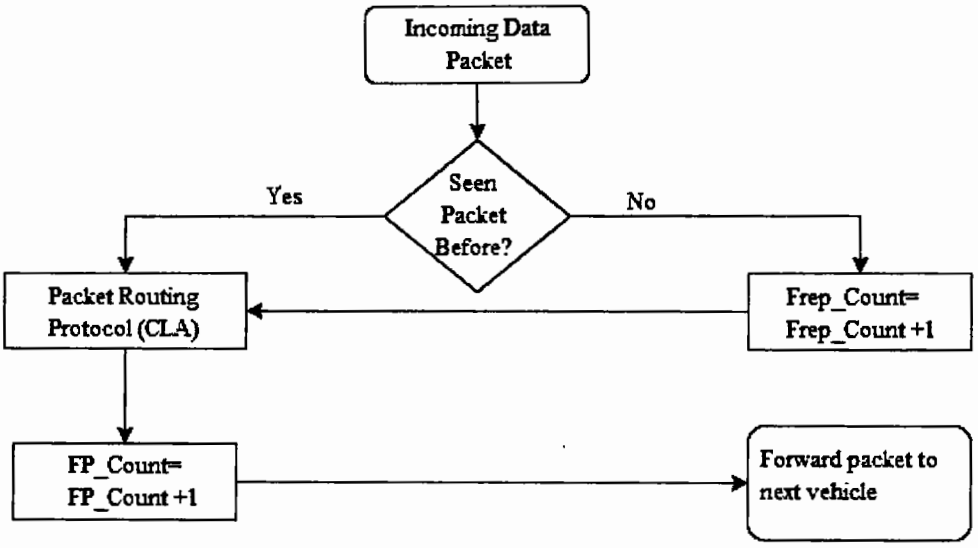


Figure: 3.5 Reputation and packet forwarding updates

3.3 Reputation Comparison

1. Comparison is made by node *j* to its own Reputation Score *(RU_j)* with respect to Reputation Score *(RU_i)* of i^{th} node.

2. If *RUj* * Threshold <*RUi*, node *j* will ask for the *RU* of its neighbor. The threshold is set to 0.8, allowing the expected difference between *i* and *j* to be 20%.

3. Calculate Average *RU* (Avg_*RU*) of the neighboring node by node *j*.

4. If Avg_*RU*>*RUi*, node *j* starts the CBMA procedure.

5. Otherwise, node *j* drive forward node *i*'s LD data packet (the flow chart of the forwarding process of LD packet is shown in Figure 3.6).

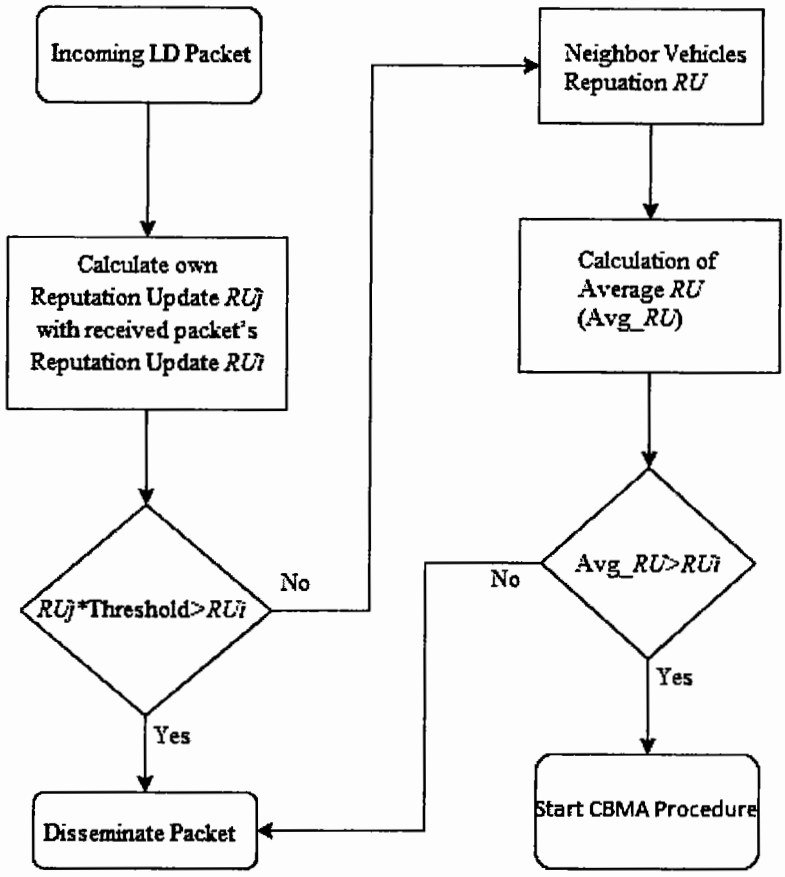


Figure: 3.6 Reputation comparison of vehicle i and j with average reputation

3.4 Combined Trust Weight Calculation

Once the reputation comparison is done, we define the value range for output value as $\Omega = \{+1, -1\}$ given such that -1 output value shows that a vehicle is malicious while +1 input value represents a trusty node. The defined data set is $S = \{(x_1, y_1), (x_2, y_2) \ldots\ldots (x_n, y_n)\}$ for each participating vehicular node. The node that exhibits properties like more neighbors, relative position, speed to the mean position, and average speed of the cluster yields the lowest weight and becomes a cluster head (CH).

Closeness to mean distance: The distance between the vehicle and the event location can be calculated based on the latitude and longitude coordinates of the GPS as:

$$D_f = arcsin(\sqrt{\sin(x) + \cos(y) + \cos(z) + \sin(w)}) \times \frac{\pi}{180} \qquad (3.3)$$

Relative speed: The speed of a node to its neighbors can be calculated as:

$$S_i = i_{pos} - \mu_{speed} \quad (3.4)$$

Node Degree: It is the number of neighbors that are within the transmission range of node, as follow;

$$E = \sum_{j \in n,\, j \neq i} (dis\ i, j) \quad (3.5)$$

Total Combined weight: Total combined weight of node can be calculated as the sum of Mean Distance D_i, Relative Speed S_i, and Node Degree E as follow:

$$W_i = D_i.wt_1 + S_i.wt_2 + E_i.wt_3 \quad (3.6)$$

Where, wt is the defined constant with values as: wt_1=0.4, wt_2=0.4, and wt_3=0.2.

Trust report about a particular vehicle in VANET, every neighboring vehicle can judge the behavior of other participating nodes. In order to generate trust report of every participating neighbor set: $\{V_1, V_2, V_3 \ldots V_n\}$ the generated reports set: $\{T_1, T_2, T_3 \ldots T_n\}$ and Judgment factor Ω: such that Ω = {+T, -T}. If S = {+T} then it indicates that the vehicle is trusty; when S = {-T} this shows negative credibility.to evaluate a particular vehicle based on the calculated reputation such as

$$C_r(Vi) = \sum_{j=1}^{k} Wi, j(V) \quad (3.7)$$

Where, C_r is the credibility of a particular vehicular node Vi, k is the total trust evaluation reports received from vehicle j, Wi total combined weight of Vi, and $j(V)$ is the neighbor node. If Cr (Vi) ≥ 0.5 the node is trusty, when Cr (Vi) < 0.5 then node is not credible. In the third case, the Trust Authority will update reputation scores in its reputation table.

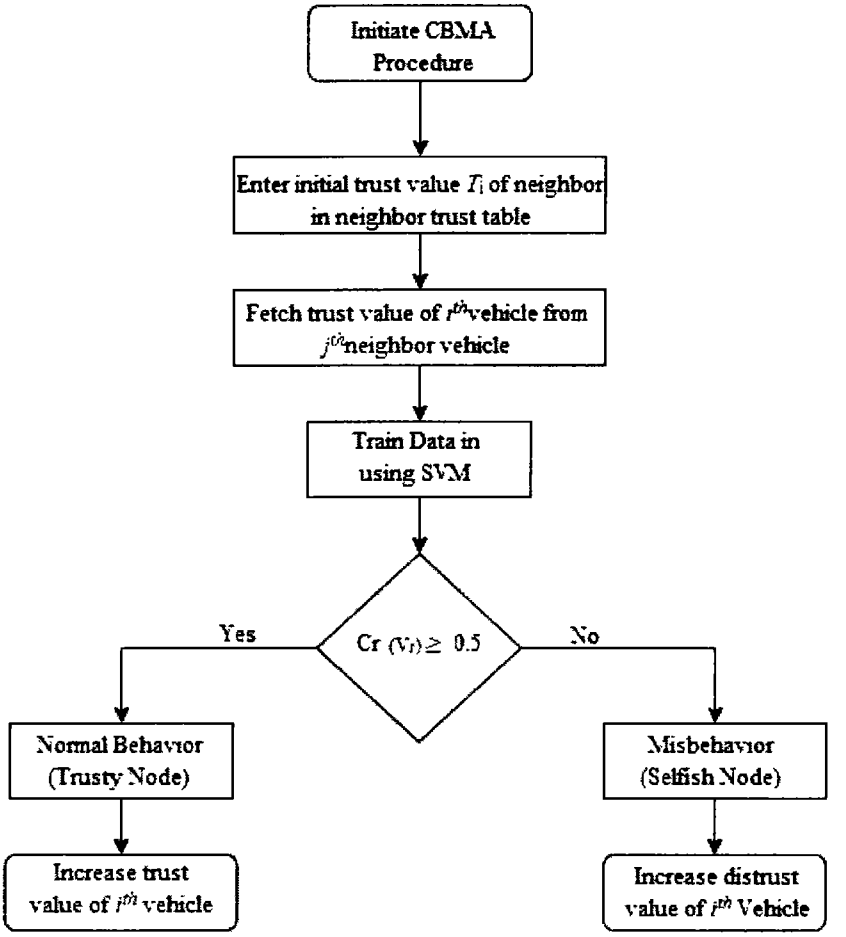


Figure: 3.7 Flow Chart of Proposed CBMA Scheme

3.5 SVM Techniques

Once the reputation comparison is computed, the next step is to classify the data based on the Support Vector Machine (SVM) kernel method. Kernal function is a course of classification for text or data analysis, and its most famous member is the support vector machine (SVM). This method is called the "kernel trick." These methods have been presented for sequence data, graphics, text, images, and vectors.

The SVM learning algorithm discovered an optimum hyperplane that divides the data sets into classes during the maximum intervals of times over the network as shown in Figure 3.8. SVM can be extended to solve non-linear hyper plane function because the set of vehicular samples cannot be separated linearly in VANET [135]. By applying kernel

functions, the samples are mapped onto a high-dimensional feature space, in which the linear classification is possible. For the nonlinear partition of the original sampling data sets, a kernel function is presented to plot the original data-sets to the high-dimensional attribute space, so that the models are linearly separated in the high dimensional attributes interplanetary.

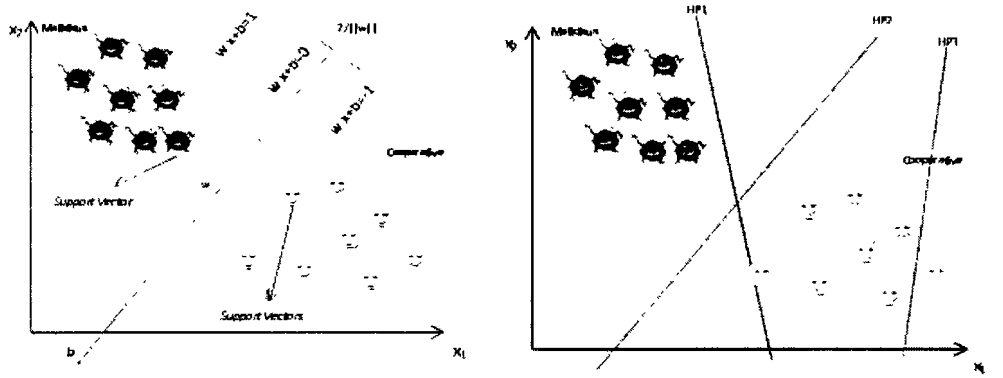


Figure: 3.8 SVM Hyper planes and Selection of Support Vectors

The support vector margins can be calculated for behavioral features can be as follow:

$$w*x_i + b >= 1 \text{ for } x_i = 1 \text{ and } w*x_i + b <= -1 \text{ for } x_i = -1 \qquad (3.8)$$

The formal equation for obtaining the optimal hyper-plane as:

$$min\{\frac{|w|}{2} + C\sum_{i=1}^{m} \varepsilon\} \qquad (3.9)$$

$$\text{Subject to } (w^T \phi(X_i) + b) \geq 1 - \varepsilon i,\ \varepsilon i \geq 0, i = 1,2,3 \ldots . m$$

Where, w is vector factor determines the direction of the kernel function; C is the number of errors considered in the trust model; m is the minimum transmission rate; ϕ is a frame of the dissemination packet; b is the partition space between kernel function (hyper-plane) and the origin; X_i is the margin; εi is the classification function for data set i. Basically, kernel functions using four classification functions for the SVM approach: namely linear, polynomial, Gaussian, and sigmoid functions. The accuracy and speed calculation

mechanism of all of these four functions are different from each other. In most of the classification scenarios, the proper kernel function is unidentified. In the proposed work, we used cross-validation to enhance parameter modification to train the sample data set. To select the promising kernel function in the proposed scheme, we used to compare the performance of mentioned kernel functions in the context of *TPR* calculation, *FPR* calculation, and *ACC* calculation. These performance parameters can be calculated as in (3.10, 3.11, and 3.12).

$$TPR = TP/(TP+FN) \quad (3.10)$$

$$FPR = FP/(FP+TN) \quad (3.11)$$

$$ACC = (TP+TN)/(TP+TN+FP+FN) \quad (3.12)$$

Where, *TPR* is the total number of true positive ratio; *FN* is the number of false negative ratio; *ACC* is the total accuracy; *FPR* is the total number of false positive ratio; *TN* is the number of true negative ratio.

Considering that the SVM approach can efficiently contract with non-linear cataloging, with the benefits of a high ratio of correctness and vigorous system performance, we implemented a data-trust prototype which is based on SVM classifier that can effectively control the true state of the alarm data based on the data contents and vehicle's properties. Second, the indigenous vehicle-trust module is accessible by using additional SVM classifiers that discover the features of the vehicle in relation of data dissemination for determining that whether a vehicular node is trustworthy and submitting a trust report to the CA. Thirdly, in order to decrease the intrusion from fake and inaccurate trust reports from the network, a Collaborative-based vehicular trust module is planned, that sums up the trust report and then gets a complete trust assessment of the assessed vehicular node.
The data-trust model builds a feature vector-based approach on the contented data sets and uses a classifier based on SVM to determine whether the message is credible. If the message is true, the proposed model will alert the driver to forward the message content across the network. If the message contents are not accurate, the proposed model sends the report to CA. The vehicle-trust model is comprised of two main modules: the local-vehicle trust module and the CA-vehicle trust module. The local vehicle trust module builds a

feature vector in accordance with the behavioral pattern of the assessed vehicle and uses the SVM-based classifier to evaluate whether it is authentic.

3.6 Intrusion Detection System

The Intrusion Detection System (IDS) is a security scheme that provides protection and protection for a variety of critical and security-sensitive networks (such as WSN, MANET, 4G, IoT, etc.) such as malicious users performing malicious attacks.

A typical IDS includes essential modules, such as information collectors, typically sensors positioned at various sensitive positions, an analysis engine that analyzes the information gathered by the sensors, and reports that record and alert when any malicious or anomalous events are detected.

The SVM based IDS model for our proposed mechanism is depicted in Fig. 3.9. It comprises a data-trust model for lowering FPR and a vehicle-trust model for the non-forwarding approach. To quickly extract distinct vector features from exchanged packets, the metrics of measurements are calculated according to the mean distance, the average speed of the vehicles, and degree of the neighboring nodes. Features filtering mechanisms and cooperative trust management approaches are presented to compute the accumulative trust weights for each vehicle. The remote sensors are used for information gathering that are mostly positioned in locations vulnerable to attack and are highly likely to be attacked. These attacks may results in leakage of juicy and sensitive information. In a VANET-like network, the position of the IDS sensor is typically the vehicle and roadside unit (RSU). The job of these sensors is to sense and collect rolling network information and send it to the analysis and detection engine, which then analyzes the information in different ways depending on the type of IDS deployed.

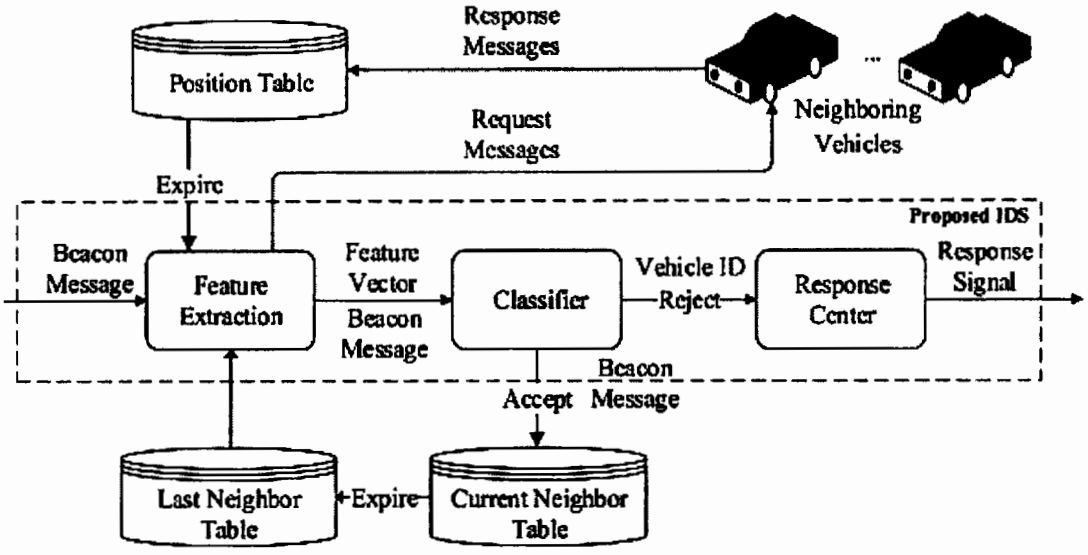


Figure: 3.9 IDS model using SVM approach [95]

Upon identifying any anomalies or malicious events, the detection engine refers a report to the reporting engine, which forwards the events to the appropriate users to let them know and take appropriate action against selfish users.

3.7 Chapter Summary

In this chapter of the thesis, we proposed cooperation based misbehavior avoidance approach integrated with trust model and data consistency model using support vector machines. To enhance the security of the proposed system, a robust intrusion detection scheme is employed to protect network from intrusions. The proposed trust model analyzed communication features which consist of emergency event information such as event reports and location verification. We also proposed a trust comparison and updating model to be consistence with supervised learning of SVM technique.

4. Collaborative-Trust Approach towards Malicious Node Detection in Vehicular Ad-Hoc Networks

Malicious node detection in VANET has always been a research hot-spot. An efficient Misbehavior detection scheme is needed to avoid and reduce the factor of selfishness and maliciousness especially in the case where the selfish beacons exploit the medium. To disseminate honest data over VANET infrastructure, it is very essential for nodes to collaborate with each other during the process of message forwarding and to ensure the successful delivery of honest data over the network. However, using the fake identities in message forwarding process easily results in the dissemination forged data over the network. Therefore, most of the existing techniques for detection of misbehavior in VANET use collaborative trust-reputation based approaches to tackle the issue forged and fake data transmission. The objective of this research is to calculate the trust weightages of each vehicle over the network and to reduce the intensity of the malicious vehicular nodes in VANET. The proposed Collaboration Based Misbehavior Avoidance (CBMA) Detection mechanism comprises data trust module and reputation calculating module, which guarantees honest data communication and reduces the False Positive Rate (FPR) of malicious vehicular nodes. The data trust module uses trust evaluation and reputation calculation model to decide whether the vehicle is trustworthy using vehicular behavior vector in the context of packet transmission. The vehicular Trust Authority uses collaborative approach to integrate several trust evaluation assessments about a particular vehicular node and formulate a complete trust assessment. The performance evaluation shows that the proposed scheme delivers more priority messages with high True Positive Rate (TPR) and low False Positive Rate (FPR). Moreover, the experimental results show that Gaussian kernel function best suits our proposed model in comparison with other rationalities. In addition, proposed models is more vigorous in context of true positive rate than existing schemes i.e. Dempster-shafer theory of evidence, majority voted model, and Bayesian inference.

In this section of thesis, we propose a malicious node discovery mechanism dependent on a cooperative trust approach, where the proposed model uses the reputation scores to distinguish each malicious node dependent on the relationship of obtained trust and reputation estimation mechanism. In this section of thesis, our contributions are as per the following:

- We analyzed the vehicular normal flow of obtaining genuine information in VANET. We presented issue definition that the best way to distinguish malicious vehicular nodes dependent on the coordinated efforts of acquired information from participating vehicles in the network. In addition, we utilize the reputation scores to procure the ratio of malicious nodes.
- We proposed a trust and reputation acquiring model for dynamic VANET dependent on a cooperative trust approach. In the proposed scheme, every vehicle chooses one of adjacent vehicles inside its corresponding range as next hop to exchange information until the information is exchanged to the desired destination vehicular node. The proposed reputation and trust calculation mechanism motivates participating vehicular nodes to adopt good behaviors and exchange honest information across the network. The proposed model shows the potential of collaborative trust approach to integrate trust and reputation score to formulate a comprehensive model for robust VANET scenario
- First, we analyzed a technique for computing malicious node impact for a dynamic VANET topology. Second, we show an exception identification technique to deal with strange information recognition. Since genuine information is discrete, we develop a twofold framework to change logical information to continuous information. Thirdly, we analyze to deal with the correlation between node discovery of exchanged information and impact of malicious nodes. At last, we make reputation estimation to assign score to each malicious data for the identification of malicious vehicular nodes. Our method provides a new model of reputation and trust calculation so that each participating vehicle can exchange and view of reputation and trust score of their neighboring vehicle.

- Implementation of the collaborative-trust approach analyzed the execution of our proposed scheme. We examined running times of estimation for impacts, identification origin of the malicious data, and malicious vehicular nodes under different ratios of the message exchange. Furthermore, for accomplishing the adequacy of the proposed model, we analyses the connection between abnormal node's impact and calculated reputation score. Implementation of the collaborative-trust approach demonstrates that the proposed scheme has shown better TPR for efficiency and safety of the network Moreover, based on the identification accuracy rate of malicious nodes; a comprehensive comparison is presented with other existing related works.

4.1 Collaborative-Trust Approaches

One of the challenging tasks in VANET is the dissemination of robust data and information across the network. Robust data dissemination is very crucial task to most of VANET applications. The traffic flow is growing steadily, especially in urban areas. Half of the world's population lives in urban areas and is estimated to rise to 60% by the year 2050. Thus it requires efficient and honest message transmission. There are many aspects which affect the performance of VANET like mobility pattern, speed of vehicle; number of vehicles etc. For illustration, VANET can give and makes advance security measures and control decisions for drivers through cooperative control innovation between vehicular nodes. In vehicular ad-hoc network, each vehicle behaves independently and exchange data with other vehicular nodes over the network. Due to this nature of independency misbehavior occurs. However, it is very challenging to detect maliciousness in regular data traffic due to advanced methods of attack. Misbehavior occurs intentionally or un-intentionally. In intentional misbehavior the attackers disrupt the normal flow of communication in VANET. While un-intentional misbehavior comes up with faulty nodes or vehicle. Because of the vast versatility and dynamic topological changes of participating vehicular nodes in VANET, the connect upkeep time span between vehicular nodes is short so that the effectiveness of network is decreased.

Drivers in VANET may apologies to cooperate by progressing information from other vehicles; this selfish behavior degraded the normal flow and performance of the network. Current VANET security principles center on the upper layers of the correspondence model and there is an absence of safety arrangements at the lower layers. Protection, verification, and secure message dispersal are a portion of the fundamental issues that should be completely tended to and addressed for the far reaching reception/sending of VANET. Traditional trust approaches suggested in [129-132], such as reward-based collaborative approaches, could otherwise not be able for resolving the problem because the partner node would deliberately become a self-serving node for rewards. In addition to selfishness, misbehavior and malicious nodes are another focus of VANET collaboration. Since the vehicle or node will send fake and deceptive information for malicious reasons, detecting such an error message is more important than identifying a node that is misbehaving. Malicious attackers also send false traffic warnings to other vehicles in VANET, causing drivers to confuse and eventually lead to traffic accidents. Eliminating selfishness is the primary design goal during Emergency Warning Message (EWM) propagation. Owing to absence of identification in Vehicular Ad-hoc Network, EWM is broadcast out for all the nodes located within certain area. Therefore, instead of multi hop route setup we adopt broadcast setup for dissemination of data. The prototype of cloud computing might be brought into VANET, in a combined structure; every vehicle is viewed as a portable mobile gadget (cloud hub) with multi-sensors. These sensors have the computing and correspondence capacity to procure valuable traffic data. Additionally, the Computer Information System Company (CISCO) used another processing idea called as fog computing, which moves registering, stockpiling and different elements of distributed computing from centered focus to the edge of organization. In fog computing, fog servers are conveyed at the edge of the network. Each server is an exceptionally high virtualization capability, like a lightweight cloud server, fog servers can give clients with information stockpiling, computing capability, and remote communications. Therefore, fog servers may give a decision metric to detect malicious traffic data. The practices of malicious nodes may cause more genuine road accidents and crashes. In this way, all types of attacks in VANET are influenced by driver's behavior, but also causing huge damages to traffic

safety. Further, in case where honest vehicular node becomes malicious, the inward nodes can be greatly affected with exchanged information, and the cryptographic techniques are hard to identify it. Therefore, how to identify out the inward malicious vehicular node by some lightweight strategies should be centered focus.

4.1.1 Behavioral Consistency Checking

Local-based detection scheme based on behavior vector depends on available data from a single node in VANET. Local-based detection scheme based on behavior vector scheme is efficient in term of detecting time as this type of detection don't have any dependency on neighbor participating nodes in network as shown in [133-135]. The mentioned schemes used cooperative watchdog models based on Dempster-Shafer theory and SVM based intelligent mechanism to detect malicious nodes. Time delay is to be considered as a well-known factor for detecting fake information over VANET. Detection schemes with a lower delay are considered as an efficient detection scheme and vice versa. All mentioned schemes in local based detection capably detect position of nodes. However, due to insufficient information from single participating neighbor vehicle cannot offer precise results for misbehavior detection in VANET.

4.1.2 Reputation-Management

The collective opinion regarding a vehicle is represented through reputation-management approach, which is based on public knowledge. It signifies a vehicle's long term behavior factors and can forecast vehicular future behavior up to some extent. A reputation management approach for pseudonym-enabled VANET is proposed to tackle with malicious nodes. We proposed service-reputation approach for identification of dishonest nodes and feedback-reputation process to deal with strategic attackers. For incentive and trust management in VANET, we presented a job market-signaling strategy. Vehicles earn credit for successfully completing network cooperation operations. This can be used to stop self-propelled vehicles as well as hostile vehicles. However, the proposed scheme did not distinguish between credible data packets in various application scenarios.

4.1.3 Collaborative Assessment

Collaborative assessment enlists the help of other vehicles to increase the accuracy of the evaluation. The main issue is figuring out how to bring disparate viewpoints together. MV,

WV, BI, DST, and neural networks are some of the most commonly utilized approaches. The majority voting system is based on the idea that the majority of cars are trustworthy and honest, and that the majority wins. Weighted voting assigns a numerical value to each vote based on the vehicle's characteristics, such as proximity to a location and reputation, and then adds up all the votes. The dynamic access service evaluation scheme is proposed, which comprehensively considers the direct and indirect service quality evaluations, can cope with the interference and effect brought by the dynamic change of network topology and node instability by introducing a time attribute, attenuation mechanism, and feedback regulation mechanism of the historical record. Most of the research suggested Bayesian inference-based vehicle trust mechanism, but did not show how to calculate prior probability and conditional probability. To aggregate cluster members' judgments for excessive or slow speeding misbehavior, we compared DST and CBMA models correspondingly. In comparison to DST, CBMA can self-learn based on previous experience, which enhances the detection rate and lowers the false positive rate. We also proposed SVM-based intelligent detection model for clustered VANET to address the discarding packet behavior.

4.2 Trust and Reputation Calculation Model

The detailed collaborative-trust based model is presented in this section. The mechanism defined for trust and reputation evaluation is presented to calculate the trust weightages of each vehicle over the network. Further, to integrate misbehavior detection and reputation calculating schemes among multi-services are also demonstrated.

4.2.1 Data Trust Model

We presented the trust evaluation approach that can evaluate trust value for a specific vehicular node as well as calculate trust weightage for a single node. The trust value for every vehicle is derived from the external and internal factors which are represented as t_1, t_2, t_3 ... t_c to calculate value, we assess the misbehaving nature of a particular node and acquire the estimated value of T_t metric for every node and each section. The derived eigenvalue e_i of t_i, $i \in \{1, 2... n\}$ can be calculated through Collaborative-trust scheme. If the ratio of $\sum_{j=1}^{p} e_j$ and $\sum_{j=1}^{n} e_j$ is closely relates to 1, all vehicular node n behavior

factors can be utilize instead of p. Collaborative trust value for each vehicle can be calculated as: $T = \sum_{i=1}^{p} bifi$ where $b_i = e_i / (\sum_{j=1}^{m} ej)$ is the ratio of information exchange for each factor for combined weight can be calculated as $W_i = D_i.wt_1 + S_i.wt_2 + E_i.wt_3$.

In order to get the estimation for position verification physical measures can be used in VANET to derive received signal strength (RSS) of the network. Malicious vehicular nodes may exchange forged information which leads to wrong calculation for RSS value. Every vehicular node observes its neighbors' RSS value over time in the network. If the resemblance is found in the calculated values then it should be communicated across the network. As discussed, nodes with fake identities have very similar RSS patterns and values. The participating vehicle will collect the RSS pattern and matches their similarities. The distance function can be defined as *D (PA,PB),* can be used to show the resemblance between two defined time series. The distance for Pattern ;A' and Pattern 'B' can be calculated using Euclide's method as follows:

$$D(PA, PB)^2 = \sum_{i=1}^{T} PA^2 + PB^2 \qquad (4.1)$$

Where, T represented extent of total time spans and PA, PB represents the i_{th} element of RSS time series in Eclidean distance. For removing the interruption triggered by a malicious vehicular node which can regulate the transmission power persistently, RSS values can be preprocessed by the given passion.

$$RSS = \frac{R-\mu}{3\delta} \qquad (4.2)$$

Where μ and ð represented mean values and deviation for derived *RSS* values. Every specific vehicular node '*A*' compares the similarity index of the *RSS* time series pattern with its neighboring participating nodes like $N_1; N_2 \ldots : N_k$, where $Ni; Nj \in N(A)$

$$D(PNi, PNj) = \frac{D(PNi,PNj) - Dmin}{Dmax - Dmin} \qquad (4.3)$$

Where, $Dmax$ is maximum value for all D and $Dmin$ is minimum range. The calculated value for $D(PNi; PNj)$ is in range between [0; 1]. If the value of $D(PNi; PNj)$ is calculated and found closer to 0, we can assume that RSS patterns are more alike. In case if the value is calculated nearer to 1, RSS time series patterns can be assumed as less similar. Vehicle B can calculate the RSS pattern as follows

$$f_l = Dmin\ (PN_j, PN_i) \tag{4.4}$$

The validity period of message is related to the type of event. For example, the validity period of emergency electronic brake message is shorter than the validity period of the traffic accident notification. The time validity of message can be expressed as $t- t' < \Delta t$, where t is the current time, t' is the time of the event, and Δt is the validity period of the message. The distance between the vehicle and the event location can be calculated based on the latitude and longitude coordinates of the GPS. Assuming that the latitude and longitude of the vehicle location is (Lng1; Lat1), and the latitude and longitude of the event location is (Lng2; Lat2). The distance D_i between them can be calculated by using (4.5-4.6).

$$D_i = arcsin(\sqrt{\sin(x) + \cos(y) + \cos(z) + \sin(w)}) \times \frac{\pi}{180} \tag{4.5}$$

Where, r is the radius of cluster.

$$\begin{cases} x = f(Lat1 - Lat2)/2 \\ y = f(Lat1) \\ z = f(Lat2) \\ w = f(Lng1 - Lng2) \\ f(x1) = x1 \times \frac{\pi}{180} \end{cases} \tag{4.6}$$

Where, f (x) converts the latitude and longitude into radians.

4.2.2 Reputation Calculation Model

An effective model can deliver useful information to recognize whether a node is reliable for the exchanging of data over the network. The second phase of the proposed model encourages nodes while acting in a good way and to restrict the nodes while acting in a bad way. In this section a comprehensive review about various trusts management mechanisms

are presented and after thorough analysis it is investigated that the dynamic nature of Vehicular ad-hoc Network makes it unfeasible in a practical scenario. We used the trust and reputation calculating model as demonstrated in section 3.1.

4.3 System Model Analysis

Collaborative-trust assessment scheme uses the reputation values of participating vehicles for improving the evaluation accuracy. The primary issue faced in the scheme was "how to integrate different reputation scores".

4.3.1 Vehicular Node behavior Analysis

In this module we examine the behavior vector of neighboring vehicles through Watchdog strategy, where vehicle defines behavior features according to the observed behavior of the network. After observation we use a SVM-based vehicular classification mechanism to differentiate vehicles in context with misbehavior detection. The scheme efficiently determines whether a neighboring vehicle is trustworthy or not. In terms of packets exchange, we deals with packets drop ratio (PDR), packets delay forwarding ratio (PDFR), packets modification ratio (PMOR) and packets misroute ratio (PMRR) to classify each node on the network. The mentioned parameters can be calculated as (4.9)

$$\text{PDR} = N_{dp}/\text{N},\ \text{PDFR} = N_{dy}/\text{N},\ \text{PMOR} = N_{cp}/\text{N},\ \text{PMRR} = N_{nr}/\text{N} \quad (4.7)$$

Where N is the the total number of data packets exchanged in network; N_{dp} show the number of drops data packets; N_{dy} signifies the total number of delay data frames; N_{cp} is the number of changed data, and N_{nr} is the number misrouted data frames.

4.3.2 SVM based Classification

To judge and decide whether a vehicle is trusty or not, SVM based classification mechanism is adopted which takes vehicular behavior as an input. The defined value range for output value is $\Omega = \{+1, -1\}$ given such that -1 output value shows that a vehicle is malicious while +1 input value represent a trusty node. For SVM approach, a data set S = $\{(x_1, y_1), (x_2, y_2) \ldots\ldots (x_n, y_n)\}$ of trained samples where x and y represented the vehicular behavior vector feature and n represents the total number of trained data set 'S' and $y_i \in \Omega$. SVM kernel function for data set S can be defined as $k(x, y)$, given that trained data sets

are indirectly projected to higher behavior feature space. Decision function can be found as:

$$\sum_j(\alpha j\, k\,(x,y) + D \tag{4.8}$$

Where, αj is represented as Lagrange multiplier, $k\,(x, y)$ denoted the SVM kernel function, and D shows the defined constant.

The participating vehicular node generates a trust evaluation report based on the SVM classification approach and secretly shares the same with Trust Authority.

To generate a trust report about a particular vehicle in VANET, every neighboring vehicle can judge the behavior of other participating node. We outline that $\{V_1, V_2, V_3 \ldots V_n\}$ is the neighbors set for vehicle V_j and $\{T_1, T_2, T_3 \ldots T_k\}$ shows the generated reports set on V_j. In the context of TA Model, the set for judgment factor Ω contains two attributes, namely $\Omega = \{+T, -T\}$. In this case +T shows that the vehicular node is performing in reliable way and -T represents that the participating node is not unreliable. Finally, we can make three propositions based on the given attributes: if S = {+T} then it indicates that the vehicle is trusty; when S' = {-T} this shows negative credibility and U = {+T,-T} indicating that the vehicular node is either trusty or malicious.

We can assume reputation score of V_j is R_e. If a set of neighbors' vehicle V_n reports that vehicle V_j is trusty. Throughout this work, if $C_r(V_i) > 0.5$ the node is trusty, when $C_r(V_i) > 0.5$ then node is not credible. In the third case, the Trust Authority will update reputation scores in its reputation table.

Mathematical form of the mentioned propositions can be as,

$$m_1(V_i) = R_e; \qquad m_1(V_i) = 0; \qquad m_1(V_i) = 1 - R_e \tag{4.9}$$

If vehicle V_n reports that vehicle V_j is not trusty, then:

$$M_2(V_i) = 0; \qquad m_2(V_i) = R_e; \qquad m_2(V_i) = 1 - R_e \tag{4.10}$$

If the TA takes k trust evaluation reports on vehicle V_j, credibility of the vehicle V_i as:

$$C_r(V_i) = m(V_i) = \sum_{j=1}^{k} j(V) \tag{4.11}$$

Where, C_r is the credibility of a particular vehicular node, k is the total trust evaluation reports received from vehicle j, m is the minimum data transmission rate, and $j(V)$ is the neighbor node.

4.4 Performance Analysis of System Model

In this section of thesis, analysis and elaboration of the proposed framework and performance parameters is given in order to draw a clear picture of the effects of different variables.

Table. 4.1 Simulation Parameters

Parameter	Value
Number of nodes	100
Map size	$1000m \times 1000m$
Mobility model	Described by IPNs
Propagation model	Two-ray ground reflection path loss model, Ricean fading model
Link capacity	c_l = 1Mbps
MAC	IEEE 802.11p
Number of sources	8
Percentage of misbehaving nodes	$0 \sim 0.5$
Maximum data rate	M_s = 1Mbps
Minimum data rate	m_s = 0Mbps
Step size	$\tau = 0.1$
Transmission power	$P_t = 1mW$
Interference Transmission power	$P_j = 1mW$
Path-loss constant	$\rho = 2.5 \times 10^{-4}$
Path-loss exponent	$\nu = 2.7$
Receiver noise	$N = 10^{-10}mW$
Node speed	$0 \sim 20m/s$
Simulation steps	1000

In the context of data trust model analysis, we used different kernel functions to evaluate the performance of SVM-based text classifier and comparison against existing techniques i.e. Collaborative Contact-Based Watchdog (CoCoWa), Majority Voting (MV), Bayesian inference (BI) and Dempster-Shafer Theory of evidence (DST). Table 4.1 depicted the simulation parameter for experimental setup. To evaluate the performance of collaborative-trust model, we can defines the performance evaluation of classifiers through different kernel functions to obtain local trust values of the vehicles, and then compare collaborative-based approach against the existing schemes

In the proposed scheme we apply linear, polynomial, Gaussian, and sigmoid functions, for choosing the best suited function for SVM analysis. To evaluate the performance and parameter tuning for SVM functions, we used cross validation approach. As shown in

Table 4.2, the SVM classifier evaluation of the linear kernel is considerably not as good as in comparison with other kernel functions, it shows the indication that it is complicated to separate the data sample. We can also observe that Gaussian kernel shows best classification accuracy with high True Positive Rate (TPR) and low False Positive Rate (FPR), so finally we choose Gaussian kernel function for SVM classification mechanism.

In comparison with DST model, our proposed collaborative-trust scheme has less evaluation parameters and more sufficient behavior features. We presented a comparison between the Gaussian function for CoCoWa, DST and CBMA schemes.

Table. 4.2 Maliciousness detection using SVM kernel approach

	Performance Metric		
Kernel Function	TPR (%)	FPR (%)	ACC (%)
linear	94.17	20.49	93.44
polynomial	95.21	18.09	94.40
Gaussian	97.80	14.17	95.27
sigmoid	95.61	19.70	93.14

Fig. 4.1 show that the proposed collaborative-trust scheme returns considerably high TPR despite of insufficient sample data sets. It is observed that the collaborative-trust scheme returns a high TPR ratio, despite of fact that how much data packets transmitted due to its stronger generalization capabilities. CBMA, DST and CoCoWa are generally used vehicle-centric decision logics for malicious behavior detection in VANET. Reputation and percentage of malicious vehicles are key performance parameter for vehicle-centric decision logics.

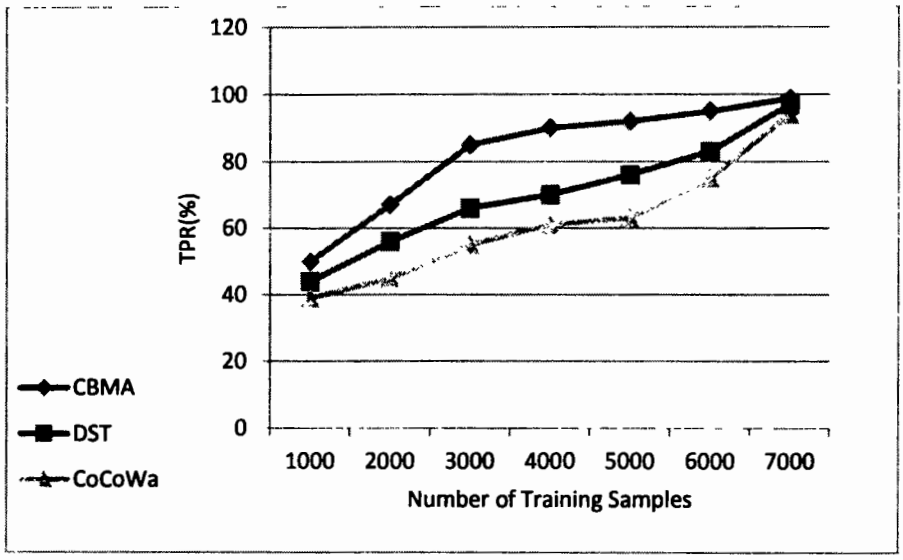


Figure: 4.1: TPR calculation based on number of training samples

Keeping in view, we define four experimental models with different reputation scores and number of malicious vehicle as demonstrated in Figs. 4.2 and 4.4 - 4.6. In the mentioned scenarios, we assumed that the prior expected TPR and reputation for all scheme is 0.01 given that the normal range for vehicle with high reputation is 0.5 -1.0. We can also assume reputation score of a particular vehicular node V_j is R_e. If a set of neighbors' vehicle V_n reports that vehicle V_j is trusty we can easily calculate credibility ratio $C_r(S) > 0.5$ for vehicle V_j. SVM based classification mechanism is adopted which takes vehicular behavior as an input. The defined value range for output value is Ω. To apply SVM approach on data set $S = \{(x_1, y_1), (x_2, y_2) \ldots\ldots (x_n, y_n)\}$ of trained samples we can easily infer from the calculated output value of Ω that a vehicle a malicious or not. Vehicular behavior vector feature can used as the judging parameters when the define range of trained samples ratio are much greater. In Fig. 4.2 as the ratio of malicious vehicular nodes reaches 30%, the TPR of CoCoWa starts decline below 20%.

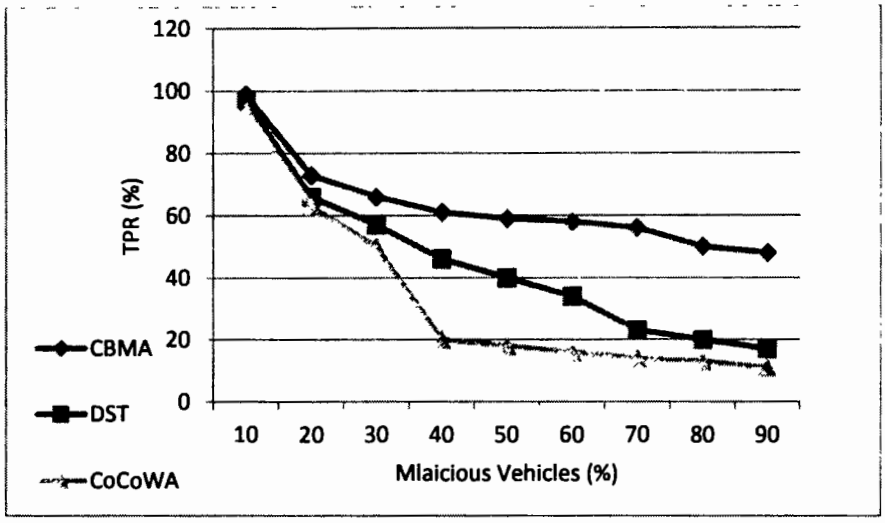


Figure: 4.2: Malicious Vehicles percentage for average reputation R_e = 0.5

This shows that in this case the scheme of CoCoWa is considerably affected by the high ratio of malicious vehicular nodes. Therefore, the TPR ratio of DST and CoCoWa will eventually decreases with the increase ratio in the percentage of malicious vehicular nodes in the network. We infer from Fig 4.2 that when the percentage of malicious vehicular nodes exceeds than 40% then TPR ratio of DST and CoCoWa begins to decrease. The proposed CBMA scheme eventually decreases when the ratio of the malicious nodes up to 23%, but remains stable till the ratio reaches 70%.

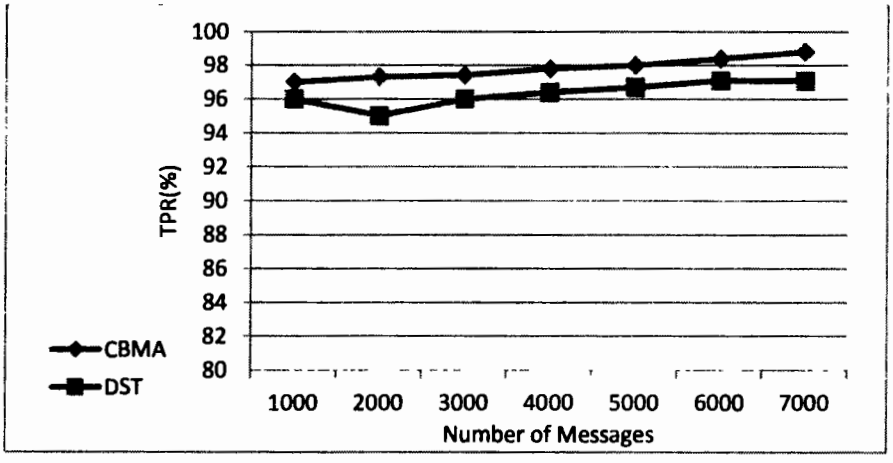


Figure: 4.3: Effect of the number of messages in CBMA and DST Approach

Fig. 4.2 and Fig 4.4 shows that the TPR ratio of collaborative-trust approach is relatively high than the existing DST and CoCoWa, and almost TPR ratio is not affected by the high percentage of malicious vehicular nodes over network. After the analysis of TPR ratio on different number of training sample and percentage of malicious vehicles we needs to analyze the effect of number of generated and exchanged message of the proposed CBMA and existing DST mechanism. As shown in Fig.4.4, the TPR ratio of BI eventually begins to decline as the percentage of misbehaving vehicular nodes increased by 0.7%. In context of TPR for DST scheme, it declines gradually in Fig. 4.3, while it remains stable in Fig. 4.4. The main reason behind this stability is that DST is affected by the high percent ratio of malicious vehicular nodes. Therefore in the expected probability derivation scenario, the percentage of malicious nodes is taken as the dominant factor for detection and performance evaluation. SVM kernel function k for data set S is indirectly projected to higher behavior feature space and TPR ratio of malicious nodes.

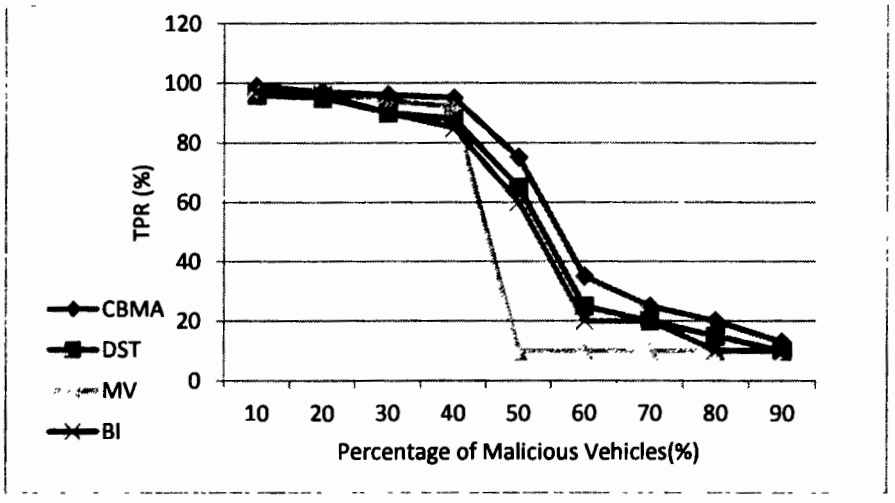


Figure: 4.4: Malicious vehicles percentage for average reputation $R_e = 0.7$

In Fig. 4.5, the TPR of BI eventually declines quickly as the R_e value of malicious vehicular nodes reaches 0.8%. In Fig. 4.5 the TPR ration of the DST and MV is in constant stable state, the main reason behind this is that vehicle cannot take voting advantages when the ratio of misbehaving vehicles is less the trusty vehicles. These experimental results shows that the behavior feature vectors presented in our scheme are significant and can efficiently detects false positive rate transmitted messages. We assumed that majority of

vehicles sending genuine and honest data over the network, and hence the true positive rate is greater than the false positive ratio of the transmitted data. The results shows that initially the percentage of the malicious vehicles are not 0, it is because of the fact due to small proportion of the vehicular density we assumed that all vehicular nodes behave honestly and no one to be found as a malicious node. As shown in Fig. 4.5, the TPR of the vehicular density in existing scheme BI is eventually degraded as the cumulative reputation of the malicious node reaches to 0.88. Keeping in view that the average reputation of malicious node for the network is 30%, all the generated messages are 30% malicious as the number of vehicles generating fake messages increases. When the ratio of the malicious nodes increases from 30% to 70%, the number of false positive factor also increases as shown in Fig. 4.6. The consequences for the forwarded messages are negative and the cumulative reputation of the vehicles decreases. The most effected scheme in this case is MV, where the higher ratio of malicious vehicle directly effect and out class the performance of the system. This is due to the reason that the nodes carry on false positive ratio as the ratio of the malicious nodes increases from 30% to 70%.

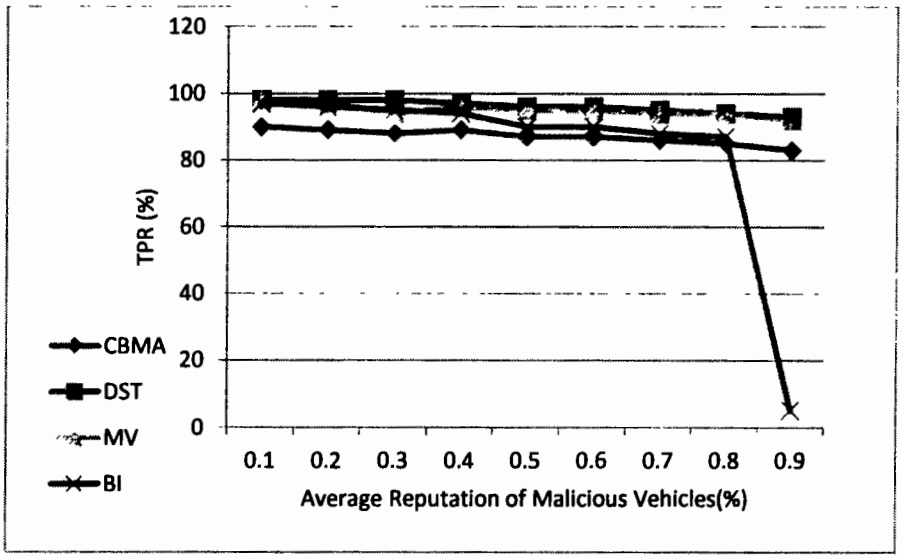


Figure: 4.5: Average reputation score for 30% malicious nodes

In Fig. 4.6 the TPR of MV is constantly in a decline state as a major portion of participating vehicular nodes are malicious. TPR of MV starts to drops when R_e value of misbehaving vehicles reaches 0.2. In the same scenario when the average reputation value

R_e reaches 0.4 the TRP ratio is drops to 0. This shows that the collaborative SVM based approach of CBMA has a higher TPR ratio, which demonstrates that this scheme is not affected by reputation scores as well as by the high ratio of misbehaving Vehicular nodes.

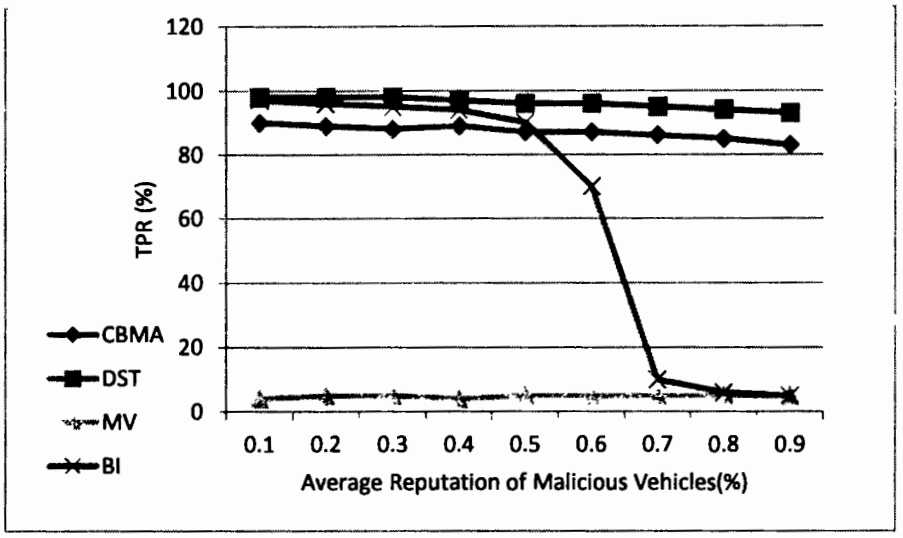


Figure: 4.6: Average reputation score for 70% malicious nodes

The experimental results also shows that the average reputation value of the vehicles reproduces their behavior factors, e.g., the situation where majority of vehicles exchange false messages and gets the lower reputation values. In contrast, the situation where few vehicular nodes exchanges false messages and gets higher reputation score.

4.5 Chapter Summary

In this part of the thesis, we proposed a Collaborative-trust based malicious detection scheme to observe fake data dissemination and data non-forwarding techniques in VANET. To tackle fake data detection, a trust model for data integration is proposed based on collaborative Approach. The proposed model analyzed communication features which consist of emergency event information such as event reports and location verification. For message non-forwarding detection, we proposed a collaborative-trust scheme converging on the behavior features of vehicles in context with data propagation. Every vehicular node uses collaborative-trust approach and SVM kernel based classification module to determine whether a specific vehicular node is trustworthy for sending the trust evaluation

reports to the Trust Authority. Trust Authority uses CBMA module to integrate several trust evaluation reports for a particular vehicle. We used Gaussian kernel function for SVM classification which best suits our Collaborative-trust scheme. Experimental results show that collaborative-trust scheme has considerably high malicious data detection ratio and cannot be influenced by the vehicular reputation scores and proportion of misbehaving vehicular nodes in VANET. After comparing with CoCoWa, MV, DST, and BI, our proposed collaborative-trust scheme is more appropriate and robust; in context of the ratio of malicious node ratio our proposed scheme shows better results. The proposed scheme shown much higher TPR ratio with different network primitives like number of training samples, average reputation score of malicious vehicles and number of messages exchanged. However, apart from detection of maliciousness there are some uncertain situations like Sybil and DoS attacks, where the proposed mechanism could be extended to avoid the unseen situations. In addition, it is very important to note down that a lot of calculations can be made by CA to get and integrate multiple trust reports. As the designing of the reputation calculation module is a significant and complicated matter, we still need to focus extensive research to tackle this issue in our future work.

5. Incentive-driven Approach for Misbehavior avoidance in Vehicular Networks

The efficient and reliable communication operation in VANET mainly relies on cooperation of participating nodes, since the existence of a single misbehavior vehicular node can affect communication interruption problems. This section of thesis proposes an effective Cooperative-based trust model to alleviate misbehaving nodes across the network, for achieving secure and reliable communication in VANET. The proposed solution addressed a wide range of security issues, comprising the detection and avoidance of misbehaving nodes, the trustworthy exchange of reputation values, and the selection of trust routes in VANET. A comprehensive cooperative-based trust (CBT) model is adopted and implemented using security and data exchange framework. In order to enhance message reliability and security in the cooperative VANET scenario, we introduced an effective key managing solution using Certified Public Key (C_{pk}) cryptographic process. The cryptographic process includes Random number (Nonce) generation, certified public key generation, encryption and decryption scheme, and digital signature. Trust module integrates direct and indirect reputation value and derive Aggregated Trust Value (ATV) in connection with key management strategies. The potential scheme is corroborated through relative performance analysis with most advanced Evolutionary Self Trust (EST) schemes and standard Ad-hoc on Demand Vector (AODV) mechanism. In order to validate the effectiveness of the proposed scheme; we investigate extensive simulations based on performance parameters of transmission delay, Packet Delivery Ratio (PDR), Effectiveness of credit rewards over network performance, Computation overhead, and Participation ratio of honest node behavior.

5.1 Incentive-driven Schemes for Misbehavior Avoidance

The pervasive computing is mostly advanced by utilizing the concept of VANET where the communicating nodes exchange data and information through cooperative based mechanism employing constrained transmission range. VANET is termed as the sub

category MANET, major applications of MANET include vehicular networking, wireless sensor networking military operations, smart homes networks etc. Vehicular networks can be more vulnerable to routing attacks due to some distinct features, like shared and unguided media, dynamic topology, decentralization of components, and constrained resource capabilities. Since the unplanned evolution of vehicular hubs shows vibrant existence and movement in network, it is very difficult to predict the topological structure of the network. In addition, due to the restricted transmission range, mobile nodes depend on other vehicles that exist in the system to transmit packets. Therefore, the normal operation of MANET requires the cooperation of a single node. Although, due to lack of unified management and the need of mutual trust between nodes in the network usually makes it a difficult task to implement secure and robust communication model for VANET. Therefore, the existence of such malicious node definitely interrupts communication operations of vehicular network [136-141].

The work presented in the proposed work offers solutions to the various restrictions of the state-of-the-art routing schemes. The proposed CBT scheme emphases on a wide range of VANET issues, such as the detection and avoidance of misbehaving nodes, reliable distribution of trust information, fairness in credit rewarding, and one-stop preservation of trusted routing.

A brief summary of the contributions made is as follows:

– Developed an efficient cooperative-based communication model, which is different from the existing routing schemes. It is suitable for any type of VANET scenario and accurately detects malicious nodes.

– Extensive working on public key generation and credit rewarding approaches has done to verify the potential of the proposed scheme, which takes into account the changes in node density, node mobility and the number of attackers, and proves the effectiveness of the CBT model.

–The proposed scheme also considers different security requirements, such as the detection and avoidance of misbehaving nodes, reliable distribution of trust information, fairness in credit rewarding, and one-stop preservation of trusted routing.

Comprehensive performance analysis is based on transmission delay, packet delivery rate (PDR), the effectiveness of credit rewards on network performance, computational overhead, and participation rate of honest node behavior.

Table 5.1: Incentive scheme approaches

Scheme	Analytical Approach
Credit-Earned	Credit scheme motivates node cooperation through rewards but High ratio of misbehaving nodes affects the performance of VANET.
Trust-Score	High ratio of misbehaving doesn't affect the performance of VANET but reputation and trust calculation results in communication overhead.
Barter-Mechanism	Personal resources can perfectly be utilized to fulfill the requirements of VANET, but a barter transaction cannot be feasible where a participating vehicle needs a certain message to retrieve but said vehicle doesn't have any the exchange unit of message which is worth more than what the vehicle wants to retrieve.
Game-Theory	High ratio of participating node results in greater probable bargaining, but the computational cost of game theory is much higher than rest of the schemes.

The proposed scheme adopts a credit-based scheme integrated with blockchain-based cryptocurrency for cooperative VDTNs. One of the most important and famous cryptocurrencies is Bitcoin. It depends on a cryptography mechanism and distributed electronic payment method; this implementation does not depend on third-party trustees. Bitcoin overlay network or simply Bitcoin system is useful in unifying a practical credit based system in VDTNs at a low cost. The main drawback of this system is of unlink ability because it is presumed every vehicle in a network has the single public key, any observer from outside can differentiate between two messages originated from the same user by tracing its fixed single public key.

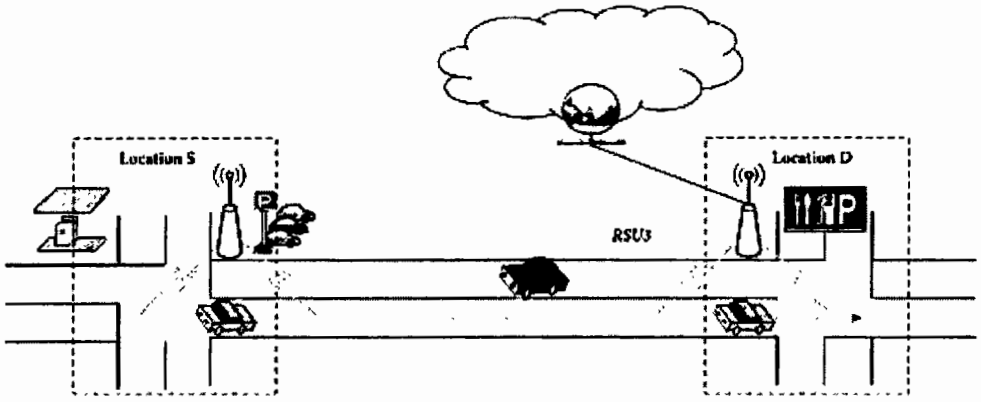


Figure: 5.1: Store-Carry-Forwarding scheme for VANET [142]

5.2 Routing Strategies

The most noticeable routing protocols used in VANET routing are Ad-hoc on Demand Vector (AODV), and Dynamic Source Routing (DSR). However, this makes the network more susceptible to routing interruptions caused by uncooperative misbehaving nodes. A promising solution to the issue of non-cooperative forwarding is proposed from the perspective of using trust-based evaluation. The option of trusting the various approaches of data computing opens up a large space of research domain. This is one of the motivating factors to make our contribution by the developing and implementing of the proposed CBT model in the framework of VANET. We proposed the most advanced trust-based routing scheme, which is said to mimic the perceptive process of humans. However, it is not possible to use trust-based routing in applications such as the VANET, where the source may not be able to satisfy its previous destination. In addition, if malicious nodes deliberately share false trust information about legitimate nodes, the possibility of failure cannot be denied.

The proposed study investigated detailed information on research analysis, classification of data, various security challenging technologies, and challenges that the research community faces in this field. Recent research work based on communication overhead, trust evaluation, energy consumption, and performance analysis to identify lightweight detection mechanism for malicious node attacks are discussed in [142-148]. The proposed

method does not depend on the size of the network, but on the selected network properties. On the other hand, in order to reduce communication overhead a probabilistic broadcasting scheme based on trust is proposed. This method depends on reducing the proportion of redundant transmissions of route request (RREQ) messages. Since the choice of this type of statistical model mainly depends on its applicability to current applications, these probabilistic methods are difficult to be universally accepted. The research work proposed in [149-154] also uses the trust model to achieve the security of MANET.

Two trust-based routing methods can be further cited in the literature, namely, reputation and credit based schemes. We also introduced a complete description of a novel encryption model that enhances the mechanism for addressing secure media to recover updated encryption keys. The proposed work uses a trust-based technique to find out the location of the vehicle with the help of the node's trust value. An improved trust-based technology is proposed to select trusted vehicle nodes and exchange messages through these nodes.

The researchers proposed reputation-base systems in which network nodes assess the trust threshold between each other and vote on the message exchange activities of neighboring nodes, thereby prohibiting non-cooperative nodes with low reputation scores from entering the system as mentioned in [155-161]. In order to encourage vehicles to actively cooperate, most of the studies proposed powerful incentive mechanisms combined with Bitcoin for the vehicular delay tolerant networks (VDTNs) to reward their active efforts as demonstrated in [162-165]. E-Sig transactions are used to ensure the fairness of the reward program, so only those vehicles can be exchanged for Bitcoin incentive transactions, provided that the vehicle has honestly completed the message forwarded to the target vehicle. The proposed work used three main prototypes of the basic model of the Internet of Vehicles. On the basis of the basic model, the classification of the basic model is analyzed; finally, the optimization effects of different variables are compared. Drivers can obtain Creditcoins for positive contributions, provided that the focus of the legend must be on the normal behavior of participating vehicles. However, CreditCoin heralds a security breach and allows dependent attacks based on the blockchain, and in a terrible case, it tracks malicious approaches to dangerous areas. In addition, the existing model ignores

those nodes in VANET that have different degrees of benefits and maliciousness for different types of exchanged data. Therefore, this solution will encounter a higher delay ratio when successfully receiving the required data content. In order to solve these shortcomings, three types of methods have been proposed, such as credit-based, reputation-based and tit-for-tat (TFT)-based incentive mechanism to encourage vehicle node sharing its data and resources are proposed in [166-174]. The above schemes focus on trust and credit evaluation to stimulate vehicle nodes to exchange content data with their neighbors by paying some credit rewards to them. For each message forwarding operation, the central agency will collect a part of the credit reward from the source node of the data packet and pay it to each communication node. It is worth mentioning that when payment is made between participating nodes, the failure of the central institution becomes a major problem

However, these solutions also need to implement reputation management systems or virtual coin management systems that rely on VANET applications. Existing work does not provide analysis and experiments to calculate the data packet transmission rate and transmission delay of the encryption function, and the number of messages realized by the 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.

5.3 System Model

The main focus of this work is to apply collaborative trust methods to avoid misbehavior of vehicular nodes in VANET, and to ensure lower packet loss rates and strong end-to-end throughput. In our proposed scheme, in order to avoid misbehavior on highways and roads, it is recommended that each node or vehicle use a certified key pair to receive a single message from each node. In order to solve the issues of message duplication, a public key-based strategy will be followed to discard and reduce unnecessary retransmissions of data packets. The vehicle-mounted node will only send and respond to the latest data base on the unique identifier associate with the specific data packet.

5.3.1 Architecture

VANET applications can be categorized in store, carry, and forward mechanism 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 Figure 5.2

(i) Service manager (SM) controls roadside units and authorizes vehicles participating in message dissemination service on VDTNs. SM issues certified public keys to the authorized roadside units and vehicles for authenticated vehicular communications and Bitcoin incentive transactions. The public key of SM for certified key generation is known to other entities in the system.

(ii) Vehicles participating in the system are equipped with OBUs embedding LTE/5G mobile communication for Internet connection, 802.11p for V2I and V2V communications [181] and navigation system with digital map. For handling Bitcoin transactions, Bitcoin client module is also installed in the vehicle.

(iii) Roadside units are under the control of SM and have 802.11p wireless link for communicating with vehicles passing by them, but not all roadside units have end to end or direct communication among them, so it is made in an opportunistic way with the help of moving vehicles.

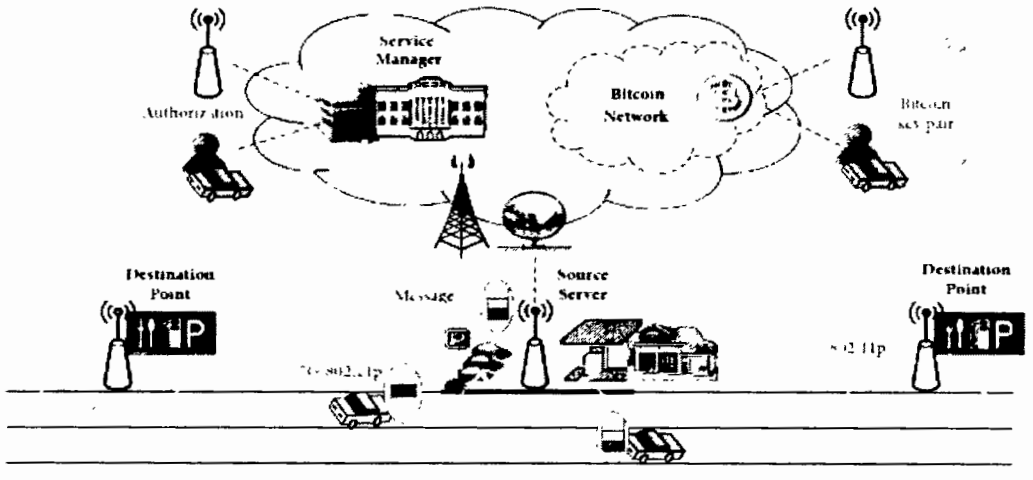


Figure: 5.2: Credit based incentive scheme for Vehicular communication [142]

5.3.2 Security Goals

We implemented certified key generation scheme for VANET 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 transmit 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 detailed security measures elaborated in Fig.5.3.

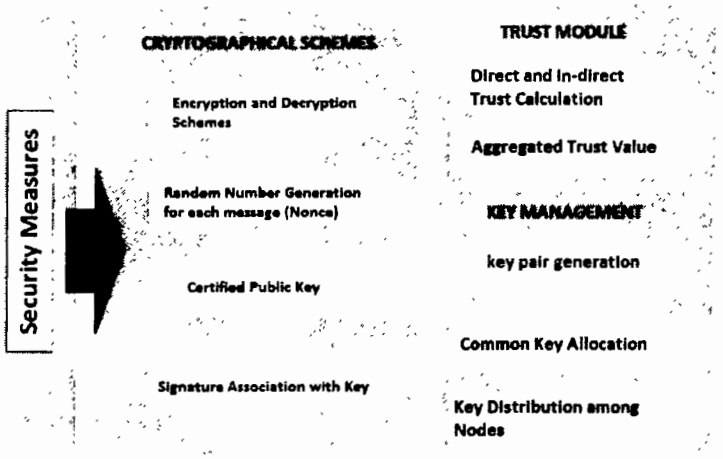


Figure: 5.3: Components of Security Model for CBT

The proposed system implements these security measures by using an authenticated public key mechanism to authorize vehicles.

5.3.3 Certified Public Key Generation using Cryptographic Scheme

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.

To calculate certified keys for Road Side Unit (RSU) and V_i, we assume that each (RSU) and Vi on VANET has a master key K allocated by the Main server. Furthermore, RSU have its own key pair $\langle KRSUi, KRSUi \rangle$ and Vi also has its pair of keys $\langle bsk_i\ bsk_i \rangle$. Additionally, let $\langle bsk_{i\ i}, V_i, RSU \in \dot{G} \rangle$ would be used as key parameters for RSU and V_i. Now, to calculate C_{pk}, let $\langle K, k, \dot{G}, \in G \rangle$ where G represent total SUM function.

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

(1) V chooses k $\in \dot{G}$ and then computes its master key $K_i =$, k, V_i then send K_i to MS and requests for C_{pk} .

(2) A random number r can be selected by MS, where $r_i \in G$, and computes $C_{pk} = K_i + r_i$ .k and $K_i = r_i + X(C_{pk}) \cdot k_i$ where X is a positive integer used for encoding function by element G. SM generated the certified keys $\langle C_{pk}, Y_i \rangle$ forV_i.

(3) V calculates $y'_i = Y_i + k_i$ $Y'i = y'_i \cdot K$ and verify that $Yi = C_{pk} + (C_{pk}) \cdot K$.

The calculated key set for $V_i \langle k_i \leftarrow Y_i, K \leftarrow Y'i \rangle$ can be used as public and master 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 $Yi = C_{pk} + (C_{pk}) \cdot K$.

We assume that roadside units and vehicles have their key pairs to receive and transmit messages. When the roadside unit or the origin server requests the participating vehicles to send a data packet to a specific destination vehicle point, the roadside unit or the origin server generates a public key pair from the master server to the participating vehicles. The roadside source server locks the key pair under the scenario that the authenticated key pair

can be used by the specific participating vehicle that can carry the data packets to the destination vehicle point. If the vehicle transmits the message to the destination with confidence and receives confirmation, it can use these authenticated key pairs.

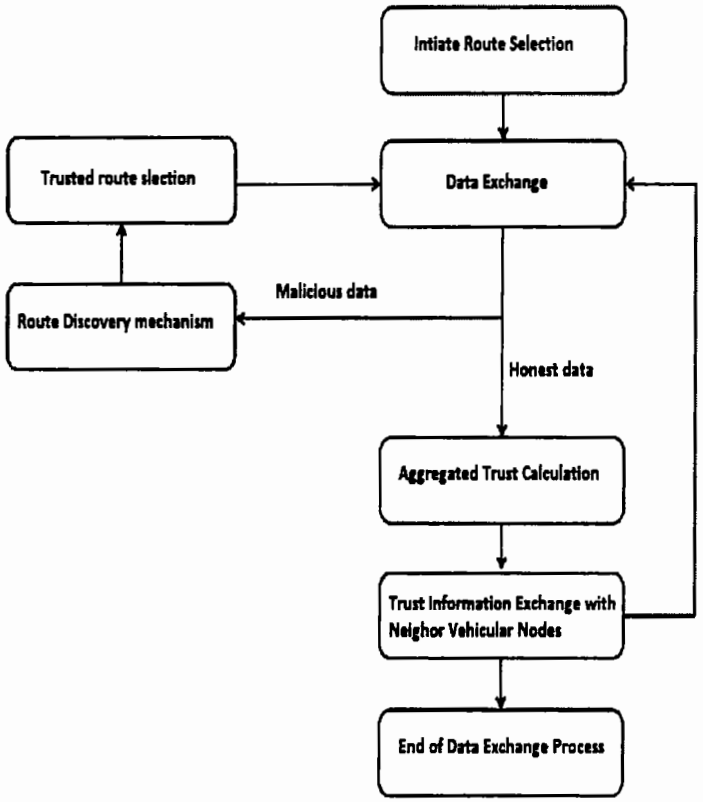


Figure: 5.4: Data Exchange Frame Work of CBT Approach

Algorithm 5.1 shows the trusted route selection mechanism of the proposed CBT scheme. Algorithm deletes the entries ID of the malicious nodes based on the define threshold values. Malicious node will be stopped from further data exchange over the network. A comprehensive report is generated against the malicious node to be sent to Main Server (MS) for intimation of other participating nodes. If the trust values associated with participating node is greater than the define threshold vallue the vehicle will be termed as legitimate node and the trusted route parameter will be associated with that participating node.

Algorithm 5.1 Trusted Route Selection

1: Begin T_r

2: V_i received data packets from V_j on route r

3: if Td < ð all data packets sent by Vi

4: V_i is encountered as a malicious node, stops from further dissemination across the network.

5: V_j removes ID of V_i from trust table entries and report MS.

6: No response to data packet sent by V_i can be entertained across the network.

6: Else V_i is termed as a legitimate vehicular node, associate the T_r to V_i.

8: Go to Step 3 of until T_r is found

9: End

5.3.4 Trust Evaluation

VANET applications can be classified through storage, carrying and forwarding mechanisms, and cooperate with participating vehicles, and the source to the destination cannot be directly linked. In order to design a robust trust integration scheme, we believe that vehicle assistance will transport some data packets received from the main server to the point of information exchange.

(i) Road Side Units (RSUs) authorize participating vehicles for message propagation services on VANET. Authentication of vehicular nodes can be done with the process of generating certified public keys 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 digital map navigation system.

(iii) Main Server (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 opportunistic approach with the help of nearby vehicles.

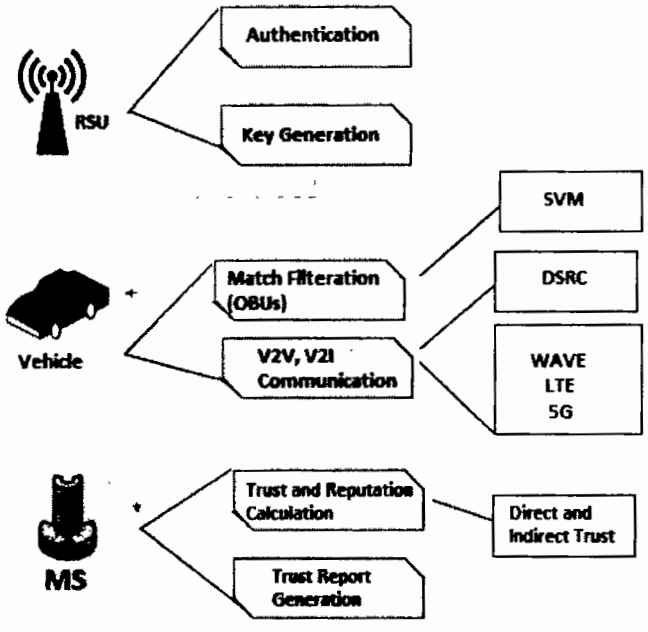


Figure: 5.5: Data Exchange Frame Work of CBT Approach

We presented a comprehensive trust evaluation model that evaluates trust and reputation value for participating vehicular nodes as depicted in Fig. 5.5. In the proposed scheme we used internal and external factors for deriving different trust values as $t_1, t_2, t_3 \ldots t_c$, we evaluate the misbehaving approach of a vehicular node and obtain the aggregated trust value T. The resulting eigenvalue e_i of t_i, $i \in \{1, 2\ldots n\}$ values are used to derive Collaborative-trust values. If the derived ratio of $\sum_{i=1}^{j} ej$ and $\sum_{j=1}^{i} ei$ is equal or nearly equals to 1, we can infer that vehicular node n adopted the behavior factor and can be used as p. Aggregated trust value for every participating vehicle can be calculated as: $T = \sum_{i=1}^{p} bifi$ where $b_i = e_i / (\sum_{j=1}^{n} ej)$ where b_i is the actual rate of information exchanged over the network.

Misbehaving node may propagate false information which indicates incorrect calculation for reputation value. Every vehicular node observes its neighbors Reputation Score R_s for a specific time interval. As disused in literature, that participating nodes retains fake identities and follow similar R_s patterns. Once the resemblance is found in R_s value pattern

then it should be announce across the whole network. The participating node collected the *Rs* pattern and checks their similarities. We can undertake that *Rs* pattern similarity, if the value calculated closely relates to 1, we can assume that *Rs* pattern is less similar. Vehicle 'B' calculate the *Rs* pattern as:

$$f_l = min_j\ Rs\ (Pni, Pnb)) \tag{5.1}$$

T (*ab*) = Node 'B' calculated trust by node 'A'.

T (*b*) = Direct Trust calculation for node 'B'

T (Σ*b*) = Summation of calculated trust for node 'B'

We can compare the calculated trust value with define threshold range and determine the following flag value of Boolean equation as

$$Td = \sum b(Pm + Pd)/Pt \tag{5.2}$$

$$\text{If } Td > ð, \text{ then } T(b) = 1 \text{ otherwise } T(b) = 0 \tag{5.3}$$

Where P*m* = Number of modified packets, P*d* = number of dropped packets, P*t* = Total number of packets, ð is the standard deviation, and T*d* denotes the trust value for node B.:

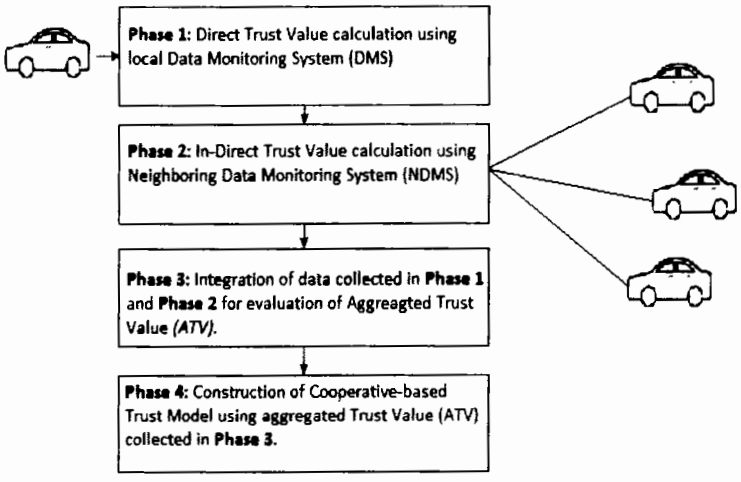


Figure5.6. Architecture of Cooperative-based Trust (CBT) Model

Algorithm 5.2 shows the reputation calculation of each vehicle in the proposed system. To calculate the reputation of the nodes *RT* function is used. RSU calls this functions and exchange event information with nearby vehicular nodes. Reputation computation integrates the direct and indirect trust values for a participating vehicular node. Algorithm derives aggregated value for the combined trust and reputation of a specific node.

Algotithm 5.2 Reputation Computation

1: Begin RT

2: Node V_j calculate direct trust values TV_j direct

3: V_j calculate indirect trust values TVj through node V_i

4: Node V_j integrate TVj trust values to aggregate trust values ATV_j

5: V_j exchange trust values ATV_j and retains in its reputation table RT

6: if $ATV_j = TLV_j$ (0.5) then

7: V sets $TLV_j = 1$ (V confirms node V_j as a honest vehicle)

8: else

9: V sets $TLV_j = -1$ (V confirms node V_j as a misbehaving node)

10: V updates its reputation table RT

11: End

5.3.5 Incentive Scheme Using Key Management

1. Key Distribution

To ensure robust and secure communication among different VANET entities secret keys have been generated, these keys should be distributed secretly to the participating VANET entities. *MS* exchange its public key with RSU, along with other key pairs generated. This messag

$$MS \rightarrow \text{RSU} : \{MS, \text{RSU}, (MS, C_{pk}), \text{RSU}, C_{pk}\,RSU / C_{pk}\,RSU^{-2})), V_i, (C_{pk}\,V_i / C_{pk}\,V_i^{-2})), C_{pk}\,V_i, , C_{pk}\,V_j, C_{pkNi}, V_{Ni})\} \quad (5.4)$$

When the RSU gets this message, it encipher it with its certified public key C_{pk}, saves its key pair (C_{pk} *RSU* / C_{pk} RSU^{-2}), the public key of *MS* (*MS*, C_{pk}) as well as those of the

corresponding vehicles (C_{pk} V_i), the RSU encrypt the message with C_{pk} and send it to the corresponding vehicle. The *RSU* sends the leader the following message:

$$RSU \rightarrow V_i : \{RSU, V_i, (RSU, C_{pk}RSU), (V_i, (C_{pk} V_i / C_{pk} V_i^{-2})), (C_{pk} V_i, V_{Ni}, C_{pkNi}), (MS, C_{pk}MS)\} \quad (5.5)$$

On the reception of message from *RSU*, V_i encipher it with the C_{pk} network public key, V_i saves all the keys of *RSU* in its register table, signify that every vehicle has a memory module by ensuring high level of security for storing key pairs. V_i sends every participating vehicular node the pair of symmetric keys, encrypted with the C_{pk}.

$$V_i \rightarrow V_{Ni}, : \{ V_i, V_{Ni}, (V_i, C_{pk}V_i, C_{pk} V_{Ni}), (MS, C_{pk}MS)\} \quad (5.6)$$

V_{Ni}, saves the public keypair for *MS*, *RSU* (C_{pk} V_i) corresponding vehicles (C_{pk} V_i). In the last phase of key distribution, i.e., when the distribution of all keys have been done, V_{Ni} will be deleted from the registry of all the corresponding vehicular entities.

2. Secure Communication through Generated Key

Next, as key distribution phase finishes, we have begun communication phase under a secure umbrella network. In order to verify the fairness and freshness of message, a T time stamp approach has to be followed.

If *MS* wants to exchange some event driven messages to its adjacent RSU, it sends message (*m*), comprising their entity identification. The message *m* will be encrypted with ($C_{pk}RSU$), upon receiving at RSU message will be decrypt with RSU private key.

$$MS \rightarrow RSU : \{MS, RSU, T, (CA, RSU, T, m), C_{pk}RSU\} \quad (5.7)$$

When RSU wants to Exchange messages with *MS*, it sends message (*m*), comprising their entity identification. The message will be encrypted with the $C_{pk}MS$.

$$RSU \rightarrow MS : \{RSU, MS, T, (RSU, MS, T, m) C_{pk}MS\} \quad (5.8)$$

At the end message *m* will be decrypted using its private key ($C_{pk}MS$). If RSU sends a message to V_i, message *m* will be encrypted with C_{pk} V_i, as follows:

$$RSU \rightarrow V_i: \{RSU, V_i, T, (RSU, V_i, T, m) C_{pk} V_i\} \quad (5.9)$$

If V_i wants to communicate with RSU, it sends message (*m*), comprising their entity identification. The message will be encrypted with the $C_{pk}RSU$. Upon receipt at RSU the message *m* will be decrypted using its private key, as well as the *T* stamp.

$$V_i \rightarrow RSU : \{ V_i, RSU, T, (V_i, RSU, T, Mes) C_{pk}RSU \} \quad (5.10)$$

If two nodes (*n,k*) belonging to the same RSU want to communicate with each other, it sends message (*m*), comprising their entity identification. The information to be exchanged will be encrypted with the symmetric key encryption mechanism as follows;

$$V_n \rightarrow V_m : \{ V_n, V_m, T, (V_n, V_m, T, m) C_{pkn,k} \} \quad (5.11)$$

$$V_m \rightarrow V_n: \{ V_m, V_n, T, (V_m, V_n, T, m) C_{pkn,k} \} \quad (5.12)$$

3. Incentive-driven Message Forwarding

In this section, we discussed incentive-based forwarding mechanism to pay reward to vehicle for successful message delivery across the network. In case, if *RSU* needs to send a message *m* to V_i through store-carry-forward mechanism with the assistance of MS. Then *RSU* demands V_i to carry out a message *m* to *RSU*, the system initiate an incentive transaction IT_x for *RSU*. If V_i successfully finishes the message forwarding process for *RSU* then incentive transaction IT_x is credited to the system network. The incentive transaction IT_x can be cashed by *RSU* using Encashment Signature (E-Sig) transaction.

In case, if V_i does not send the message *m* to *RSU*, *RSU* will lose its incentive. Once IT_x is credited to the system, the *RSU*'s input value of IT_x is termed as consumed in the incentive scheme. To handle with this condition, we set time-stamp T_s condition locked with E-Sig

for *RSU* to draw the incentive from IT_x. This scheme is suitable in case where V_i deliberately not to forward the message earlier than the time-stamp lock condition expires. **Algorithm 5.3** 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 5.3 Incentive Awarding

1: ***function*** *CreditRew (ContributorID (CID), RecipientID (RID), Credit)*
2: ***Get values:*** *ContributorAccBalance, Recipient AccBalance*
3: ContributorAccBalance = RecipientAccBalance
4: RecipientAccBalance = RecipientAccBalance +amount
5: ***emit*** *CID, RID, amount*
6: ***end***

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

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

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

(3) *RSU* verifies the signature Ω as (bpk_iV_i, Ω) by deriving V_i's public key bpk_iV_i from $C_{pk}V_i$ as calculated in Section D. After verification if the signature found valid, *RSU* formulates incentive transaction T_x1 and combines a message $msg1 := \{m\| T_s \|Sig(bsk_i\ RSU, m\| T_s), C_{pk}\ RSi, IT_x1\ \}$.

Incentive transactions for crediting and reclamation amount as incentives can be stored in IT_X1 . where $IT_X1.in$ specifies credited amount received from *RSU*'s MS pool. V_i recorded the amount given as incentives in $IT_X1.out$ and the reclamation condition for $IT_X1.out$ is

described by using script-locking containing of 2-of-2 E-Sig for V_i and time-stamp constraint for *RSU*. At last *RSU* publishes the IT_x1 to the incentive network and delivers $msg1$ to V_i.

(4) As V_i received $msg1$, V_i calculates *RSU*'s certified public key from $C_{pk}RSU$, which is then used for verification of *RSU*'s signature. The message is now stored and carries to the destination point *RSU* by vehicle V_i. Moreover, V_i initiate a validation check of IT_x1 using incentive network and generate transaction IT_x2 to claim the amount specified in $IT_x1.out$. To claim the amount, Vi verify the transaction IT_x2 excluding E-Sig unlocking script of transaction $IT_x2.in$.

(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 target location and recognizes *RSU*, V_i constitutes the another message $msg2 := \{m\| T_s \| Sig(bsk_i\ RSU, m\| T_s), C_{pk}\ RSU, IT_x2\ \}$ and exchange the same with to *RSU*.

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

(8) As to acknowledge the message delivery of V_i, *RSU* generates transaction IT_x2 and generates a partial signature to unlock 1-of-1 E-Sig script. This signature can be used by V_i to spend the amount claim in the preceding transaction $IT_x1.out$. The generated signature { IT_x2, $Sig(bsk_iRSj, IT_x2)$, $C_{pk}\ RSj$ }can be provided to V_i by *RSU* .

(9) V_i calculates *RSU*'s public key from C_{pk} *RSU* to verify the signature { IT_x2, $Sig(bsk_iRSU, IT_x2)$, $C_{pk}\ RSU$ }. If the signature is valid, V_i finalizes 2-of-2 E-Sig unlock-script by appending V_i signature with IT_x2. Finally IT_x2 will be published to the incentive network to en-cash the amount given by IT_x1 to V_i's account.

The validation process can be started on transactions IT_x1 and IT_x2 over the incentive network, upon successful validation the transactions IT_x1 and IT_x2 will be appended to the block-chain network. As a result, V_i can get credited amount as incentive for its volunteer cooperation for message propagation on VANET. The most important aspect of the 1-of-1 E-Sig lock-script is that it cannot be accomplish alone by V_i. Therefore V_i will not be

rewarded if it stops message forwarding even if IT_x1 is already published to its account in step 3 because V_i cannot solely achieve 1-of-1 E-Sig lock-script. As soon as *RSU* finds that T_x1 is not cashed by V_i after the time-lock expires, *RSU* freeze the transaction $IT_x'2$ to publish incentive because V_i did not forward the message *m* to the actual destination point *RSU*.

Algorithm 5.4 shows the data transmission phase, used after verification of the signatures of every vehicle. *RSU* generate incentive scheme for exchange of data across the network.

Algorithm 5.4 Data Transmission Phase using Incentive Approach

1: Begin

2: Set $IT_x = 1$

3: V continues data transmission along the trusted route selected in ***Algorithm 5.1****.*

4: If $Td < \delta$ *for* V_i

5: V_i *invokes* ***Algorithm 5.1*** *to execute trusted route selection phase.*

6: Else repeat Step 3

7: if msg1 sent across the network

8: V_i *invokes incentive awarding* ***Algorithm 5.2****.*

9: V_i *exchanges the Incentive Transaction* IT_x *with destination node.*

10: V_i *sets* $IT_x = IT_x + 2$

11: if $IT_x > 50$ *then*

12: V_i *has reached maximum limit of rewards*

13: else

14: Go to Step 3

15: end if

5.4 Experimental Results and Discussion

In this section, we assess the evaluation parameters and elaborate to acquired exploratory outcomes exhaustively. Our presentation assessment has three major phases:

I) To encourage node commitment in the message conveyance and to show the necessities of the motivation scheme.

ii) To confirm the practicability of the proposed motivating force plans.

iii) To examine the enhancements of various framework boundaries on the incentive driven approach to detect and avoid misbehavior.

5.4.1 Simulation Setup

The performance of the proposed CBT Model is presented in this section. We show the average Packet Delivery Ratio, Transmission Delay, Incentive impact on total number of messages and Time to Live, Average reputation, Participation ratio, and computational cost. The simulation parameters in the experimental setup are depicted in Table 5.2.

Table 5.2: Simulation Parameters

SIMULATION SETUP	
Parameter	**Values**
Area	1000-1500 meters
Number of mobile nodes	18
Cluster area	r 100 m
Data packet size	1KB
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

5.4.2 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 disseminated timely.

In Figs. 5.7 and 5.8, the effects of misbehavior vehicular nodes on the trust assessment of VANET are examined in the circumstance where no motivating force collaboration is carried out. In the simulating environment, an acting misbehavior node will just sent its

self-made messages and refused to forward those made by other vehicular nodes. Fig. 5.7 portrayed the effect of the acting misbehavior node on Packet Delivery Ratio (PDR). The decline line in Fig. 5.7 shows the decline inclination of the PDR as the extent of misbehavior nodes increased. At the start we expect that all participating vehicles are honest, i.e. the proportion of misbehaving vehicles is comparable to 0, and the PDR value can be approximately 70%. In case when the proportion of misbehaving nodes reaches 70%, the PDR value eventually declines to only 20.

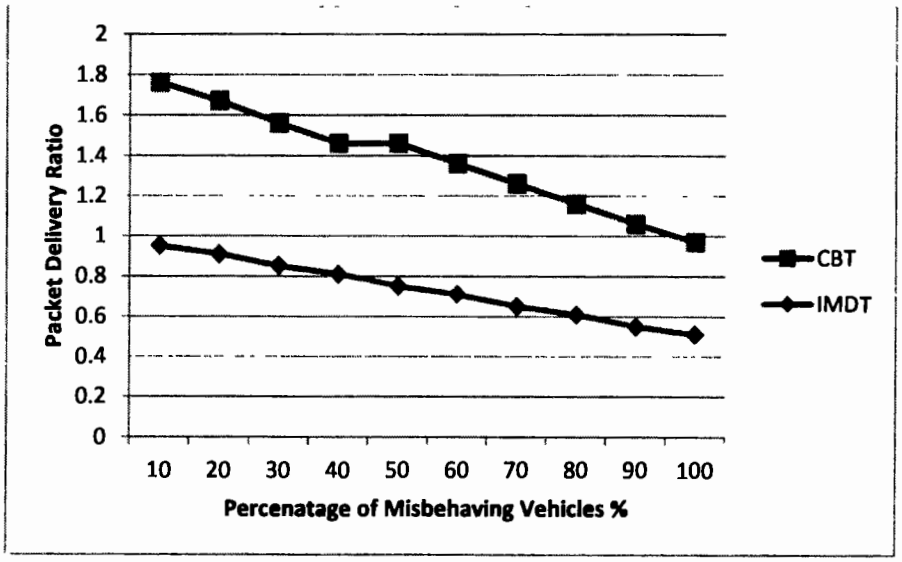


Figure: 5.7. Packet delivery ratio for different percentage of misbehaving vehicles

Fig. 5.7 depicted the deterioration inclination of the PDR relative to honest nodes. The graph represents the decline rate of the PDR when a large number of misbehaving nodes exist in VANET. Fig.5.8 depicted that as the proportion of misbehaving vehicles increases, the transmission delay will raise exponentially.

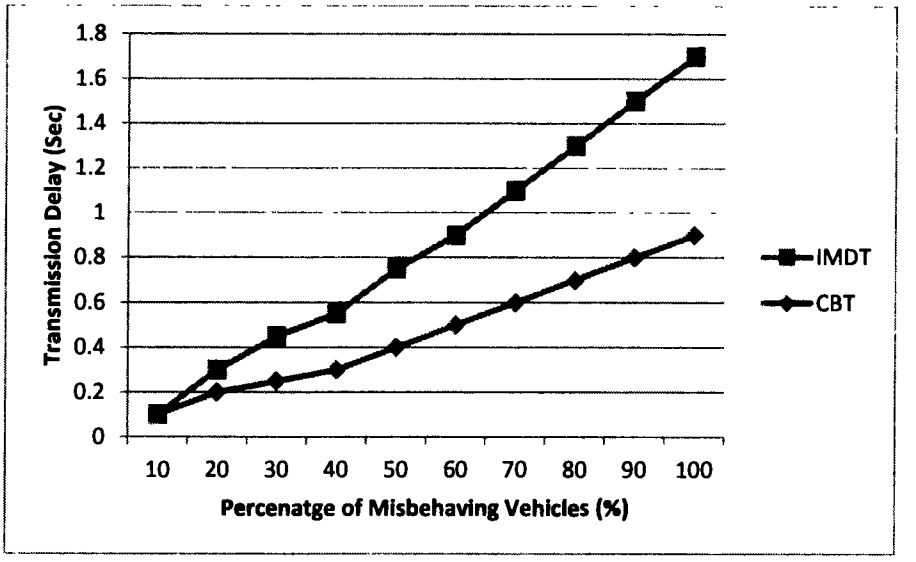


Figure: 5.8. Transmission delay under different percentage of misbehaving vehicular nodes

As portrayed in Fig. 5.7 and 5.8, the presence of the malicious nodes will ultimately drop down PDR value and rise transmission delay. Consequently, message exchange can be significantly influenced by high extent of malicious nodes, and it is exceptionally needed to present the cooperative trust and reward based approach to inspire malicious nodes for forwarding messages packets across the vehicular network. Fig. 5.9 illustrated the relationship between credit rewarded and total number of message exchanged of the proposed scheme.

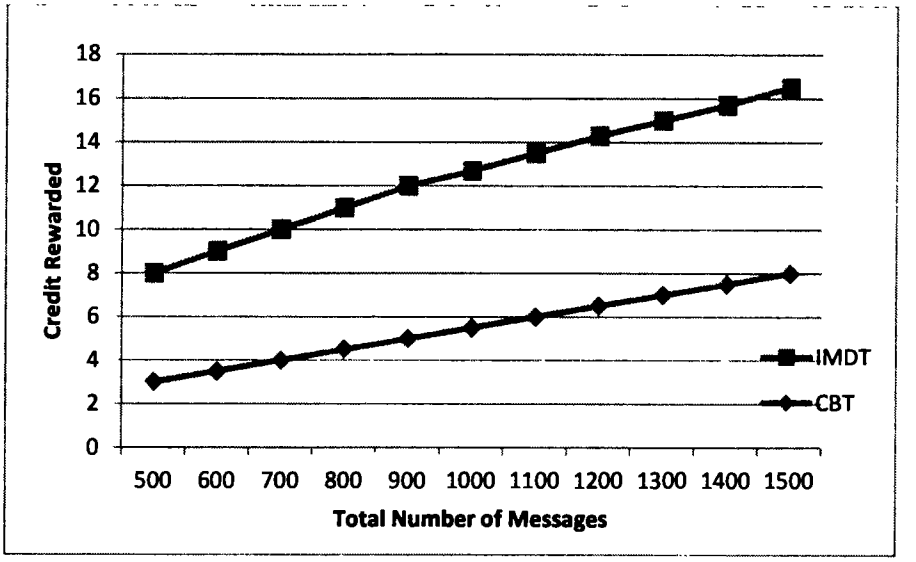


Figure: 5.9. Total rewarded credits for different number of generated messages

It is very clear from Fig. 5.9 and 5.10 that increase in the number of created packets, the accumulated compensated incentives will escalated intensely with the high proportion of exchanged packets at the target point. As shown in graph that in our proposed Cooperative Based Trust (CBT) approach, the aggregated rewarded credits are much less than that of Incentive-based Misbehavior Detection and Tolerance (IMDT) scheme. Moreover, the average rewarded incentives in the proposed CBT approach are much higher than that of the existing IMDT approach.

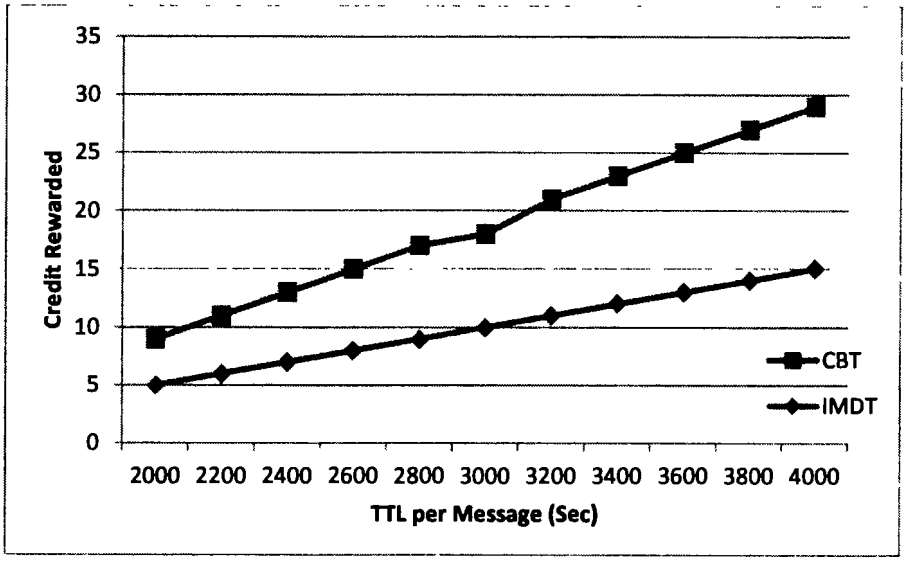


Figure: 5.10. Total rewarded credits under different number of TTL per message

Fig. 5.10 described the TTL impacts of the exchanged messages in context with credits rewarded; TTL shows fluctuation from 2000s to 4000s in the proposed model. The possibility of the absolute number of rewarded credits and average credits rewarded is comparable as shown in Fig. 5.9. Nodes cooperation plays a vital role in the rewarding mechanism of the credit to the honest nodes. As the total cooperation time increasing; TTL values is exponentially increased for participating nodes in message forwarding process. We can say that TTL values are directly proportional to the number of delivered messages. TTL ratio and its impacts on rewarded credits of the proposed scheme are represented by red line curve in Fig. 5.10. Similarly, the rewarded credits of the IMDT approach are substantially less than that of the proposed CBT approach.

Furthermore, we examined the outcome of the average reputation with constant value Ω; Fig. 5.11 relates the decisive effects about the average reputation with two define values of Ω and ratio of malicious nodes.

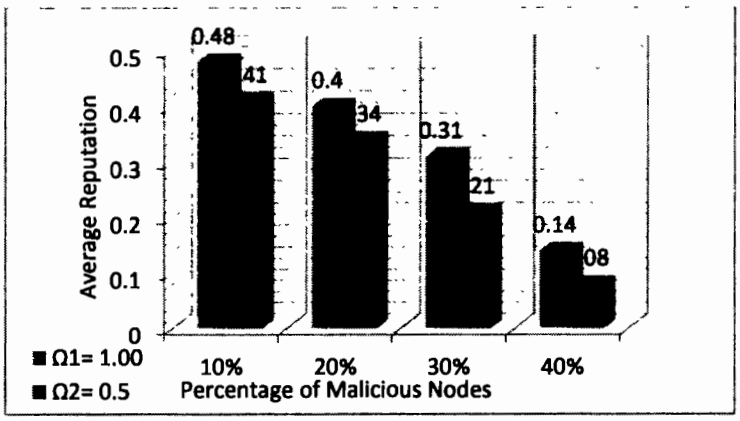


Figure: 5.11. Malicious node ration and effects on average reputation

All the results were almost positive; it is due to the fact that the number of nodes getting input in response to sending messages is much higher than the number of vehicle getting disapproval in response of creating messages.

The results appeared that average reputation is affected by Ω; the four tests results in almost average reputation with Ω = 1.00 are greater than for the four tests with Ω = 0.5. This may be confirmed on the basis that the weightage given to the forward message on the network; whereas the reputation weightage given for the creating messages is low.

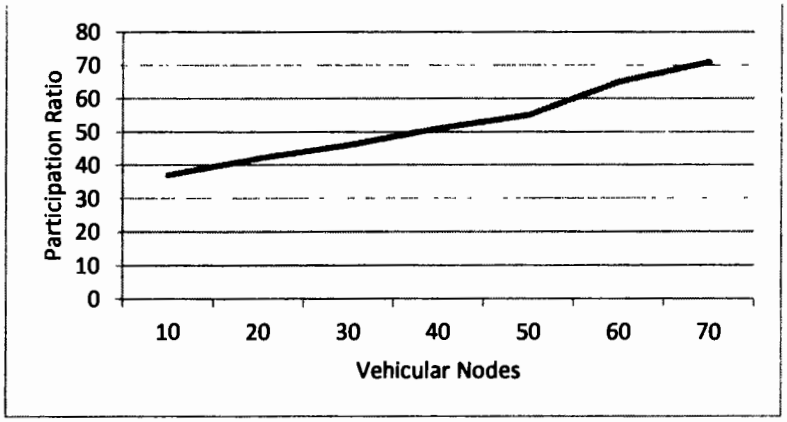


Figure: 5.12. Effect of Total Number of Cooperative vehicular nodes over participation ratio

Since a huge number of nodes receiving negative feedbacks in reaction to form and surge fake messages in the network. Fig. 5.12 signifies the participation ratio of the vehicles within the VANET.

The vehicles show up to be cooperative when they get credit rewards for their collaboration, due to this factor we can see an exponential increase in collaboration. As shown in Fig. 5.12, the node participation rate is directly effected by the total number of cooperative nodes in the network.

Fig. 5.13 showed the computational cost or computational time to create different numbers of certificates for each vehicle. Two major mechanism can be followed to create certificate are digital signature and a pair of public key key generation. The graph show that computational time is diretly proportional to the number of created digital certificates.

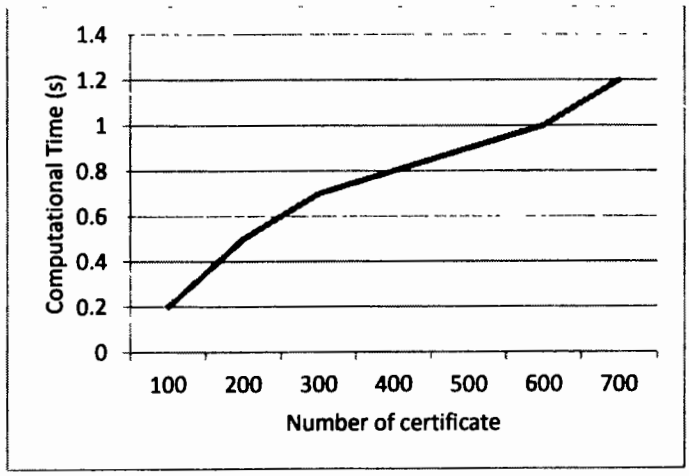


Figure: 5.13. Total number of certificates and derived computational overhead

5.5 Chapter Summary

In this Chapter, we proposed cooperative-based trust scheme integrating with comprehensive credit rewarded scheme using certified public key for VANET. Vehicular reputation can be assessed using collaborative trust evaluation approach; trusted route selection mechanism is adopted to ensure reliable communication pathways. The proposed CBT scheme employed incentive driven message forwarding approach to motivate vehicular node for their honest cooperation in the network. In order to avoid node from misbehaving, a stimulus approach is adopted where vehicles can get rewards for their

volunteer efforts and positive cooperation with other vehicle on the network. In proposed scheme, fairness and security can be guaranteed by using E-Sig 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 secure communication, we also employed Incentive Transaction Lock and unlock scripts integrated with time-stamp locked condition to deal with security aspects of the communication. Furthermore, in contrast with the existing schemes, our proposed cooperative based scheme shown better outcome for transmission delay, Packet Delivery Ratio (PDR), Effectiveness of credit rewards over network performance, Computation overhead, and Participation ratio of honest nodes.

6. Reputation Driven Incentive and Punishment Approach for Avoiding Congested Traffic

Generally speaking, misbehavior can be defined as any behavior that deviates from regular functionalities, which may be unintentional, that is, due to system failures, transmission inaccuracies, node mobility. While in intentional, selfish/malicious vehicular nodes want to take benefit of definite situation. intentional misbehavior may be recognized in order to protect their own means (such as CPU, memory, battery), not to forward those data packets which are not directly related to them and Maliciousness of nodes that wish to damage and destroy the smooth operation of the network. Depends on the total number of misbehavior nodes and the strategies adopted, throughput may be reduced, and network partitioning may occur at the same time. In any case, misbehavior of nodes will significantly reduce network performance.

The exchange of digital and encrypted signature certificates can be used to protect the basic network operations of VANET. Though, the proposed model containing encryption schemes is considered complex and resource-intensive. In this regard, cooperative-based mechanism (a common term used for such methods) are gradually being seen as a practical alternative to provide a "softer" layer of security for these networks. Therefore, the success of these systems depends to a large extent on the trust mechanism, which establishes the necessary trust relationship between related parties so that they can automatically adjust their strategies to adapt to different planes of cooperative mechanism and trust.

Louta and Bellavista [175] demonstrated that future communication system will become more and more multifaceted, linking thousands of heterogeneous devices with different functions and various network technologies connected to each other. The purpose of this connectivity model is to provide users with ubiquitous information access and advanced services. Generally speaking, the cooperation- based implementation techniques of wireless ad hoc network are divided into two categories: (a) Shaping trust through reputation scheme and (b) credit-based approach.

Resnick et al. [176] investigated reputation schemes that builds trust through the use of learning from past vehicular communication history or experience, so as to obtain the reputation value of VANET participants in the form of reputation scores based on observance, past historical communication, and opinions/opinions of other entities in the network .

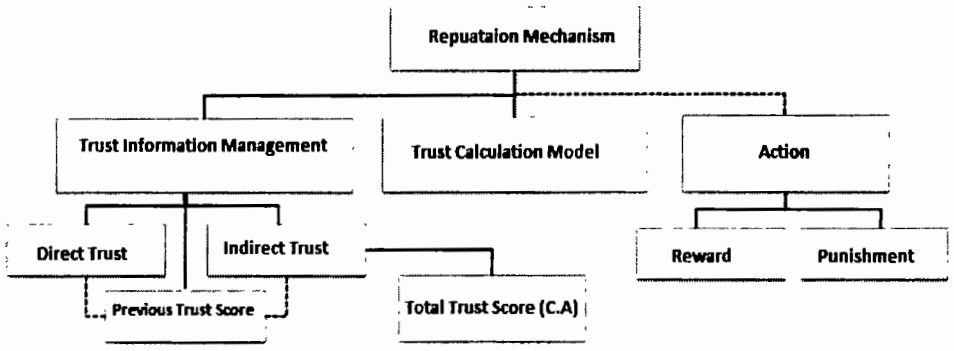


Figure: 6.1: Integrated trust and reputation mechanism

The classification of existing reputation schemes appearing in the literature are shown in Figure 6.1. It can be seen that the reputation-based scheme supports an effective approach for evaluating the reputation of other nodes in the network represented by reputation rating evaluation.

Selfish nodes in different research work have different behaviors. Dini and Duca [177] believe that selfish nodes do not want to spend their resources to forward data packets belonging to different nodes; they claim that selfish node work hard to be unattractive so as not to be selected as potential forwarder. However, if they are selected, they will forward the packet. Chen et al. [178] and Zhu eta al. [179] differentiate selfishness is as follows: individual selfishness, where each node shows the same level of selfishness to other nodes; and social selfishness, selfish nodes show different degrees of selfishness for different groups. Chakchouk [180] stated that VANET relies on node's cooperation to achieve routing function to forwards packets over the network. This fact increases the sensitivity of network performance to node misbehavior.

6.1 Reputation Driven Incentive Schemes

Trust and reputation mechanisms are multidisciplinary concepts and existed before the electronic age, these terminologies signifies a well-researched field. In recent years, various trust and reputation models with advanced characteristics have been developed in many fields. Various research fields in Information and communication (ICT) such as ubiquitous computing, ad-hoc networks, internet of things, cloud computing, wireless sensor networks used the trust and reputation integration approaches in the literature [181-187]. However, there is a lack of continuity, because there is no universally accepted set of principles to establish a trust and reputation system.

There are general investigative articles on reputation and trust approaches. Ruohomaa [188] and Trifunovic [189] surveyed trust approaches in detail, and outlined three features of trust: the conceptual trust approach, the trust calculating model, and the trust data model. Many related surveys focus on incorporating social factors into the design of VANET.

Wei et al. [190] conducted a comprehensive survey of current social aware routing protocols that use social relations for designing effective routing protocol. As mentioned earlier, although most delay-tolerant network routing algorithms assume that nodes are willing to forward messages for others, the impact of selfishness on performance is described as an interesting research challenge. In most of the cases, the node may abandon data packets received from people who have no social relationship with it. At the same time, they refer to some that consider reputation based schemes or incentive based methods. the author reviews the social characteristics of delay tolerant networks, and discusses the social based routing methods proposed in recent relevant research literature, using positive social characteristics (such as relationship, good ties, centrality) or negative Characteristics, such as selfishness.

Moreira [191] focused on using social information obtained from opportunistic happens to improve social awareness programs for data forwarding. Provides an updated taxonomy for opportunistic routing, the scheme includes sub-categories related to social aware mechanism, which can be further categorize into community-driven detection, shared-interest approach, node-popularity mechanism, and user-dynamic behavior at different

time intervals. However, the author did not mention any issues regarding selfish-behavior, cooperative-behavior and incentive-driven approach. Hoffman Et al. [192] investigated attacks and defense approaches in the trust-reputation schemes, classifying different attacks into: self-propagation, whitewash, slander, and denial of service categories. Kerr and Cohen [193] implemented avoidance strategies against some established trust schemes, proving that all verified schemes are vulnerable to at least one group of planned attack from untrusted participant. Josang and Golbeck [194] demonstrated nine diverse types of attacks on trust and reputation systems are discussed, and a set of standard indicators for measuring the robustness of trust schemes. Generally speaking, reputation-based systems are considered to maintain rational cooperation and serve credit-incentive for honest behavior, because honest players will be rewarded for its cooperative efforts. Dishonest nodes get punished and the reputation scores will be treated as analysis metric for future communication. Jian et al. [195] and Sharma [196] suggested pricing and credit-based approaches that provide credit-incentives for cooperation through charging and rewarding service use and delivery. On the other hand, nodes will receive negative credit-rewards for any misbehavior to prevent them from doing so. Jesudoss et al. [197] demonstrated three system parameters of each node's; fix budget payments, participant node payment and watchdog payment are controlled by central authority. As far as we know, there is no previous research work focused on trust-based cooperative approach in the context of VANET. Next, we categorize and discuss the issues and challenges close to the trust-based cooperative misbehavior avoidance scheme, and propose and analyze the major issues involved in its design. Security is a major concern in vehicular networks for reliable communication between the source and the destination in smart cities [198]. Today, data can be shaped in form of safety or non-safety messages with different formats like text, audio, images, video, etc. These exchanges of information between the two parties require updating the communication data by analyzing the trust value (TV).

VANET has many security loopholes and subject to a number of security vulnerabilities due to the use of wireless communication channel. The existing misbehavior node detection schemes cannot offer reasonable and robust security performance due high delay and low density in VANET. As shown in the literature review that most of the schemes are

affected with computational overhead and latency constrains. When a malicious vehicle or RSU can assume multiple identities, it poses one of the most serious threats to the survival of such networks. VANET is vulnerable to a range of attacks due to lack of dynamic infrastructure [199].

6.2 System Model

In this section, we discussed the path retention policy, reward and punishment policy, and traffic policy of the proposed system model.

6.2.1 Vehicular Architecture

The Path Reservation Center (PRC) is a managed server that configures the traffic and path reservation mechanism. It preserves the Road Reservation Matrix (RRM), which holds information about the free and reserved traffic in different time intervals.

The roadside unit (RSU) acts as entryway that links the vehicle to guided medium through internet. Usually, RSUs are deployed near intersections and are connected to each other through guided media.

In order to communicate with RSU and PRC, all vehicles are equipped with Dedicated Short Range Communication (DSRC) equipment implanted in vehicle On Board Unit (OBU). The vehicular nodes also fitted with navigation system mainly a GPS enabled digital route map.

6.2.2 Path Reservation Policy

To avoid congested routes on urban roadways, roadways capacity is distributed into two segments. The first segment can be kept for free of cost routes. When the free of cost routes are fully reserved, vehicular nodes that select to use free routes needs to charge a definite amount of Credit-Coin for reserved roadways. Roads are reserved on a first-come, first-served basis. In other words, roads are reserved for the first vehicles expressing their willingness to use them. Upon joining the network for the first time, each vehicle sends a route request to the RSU, which contains the GPS coordinates of its source and destination. The RSU calculates the shortest roadway and the free path from the source to the destination according to free of cost route quota. The RSU used arrival time of each vehicle for both pathways, so the RSU can calculate the predictable traffic stream of each roadway for various time intervals.

6.2.3 Reward and Punishment Policy

The proposed scheme is based on PRC policy, the PRC policy guarantees that the roadways are within its route quota. According to PRC policy, the roadways must be within the quota capacity designated to each vehicle by RSU. Any violation to PRC policy and reservation mechanism will lead to traffic congestion. Therefore, vehicles that break up the PRC policy and reservation process and move on the road without prior PRC Policy will be deducted from the T-credit coins balance or subject to other legal penalties by the central authority.

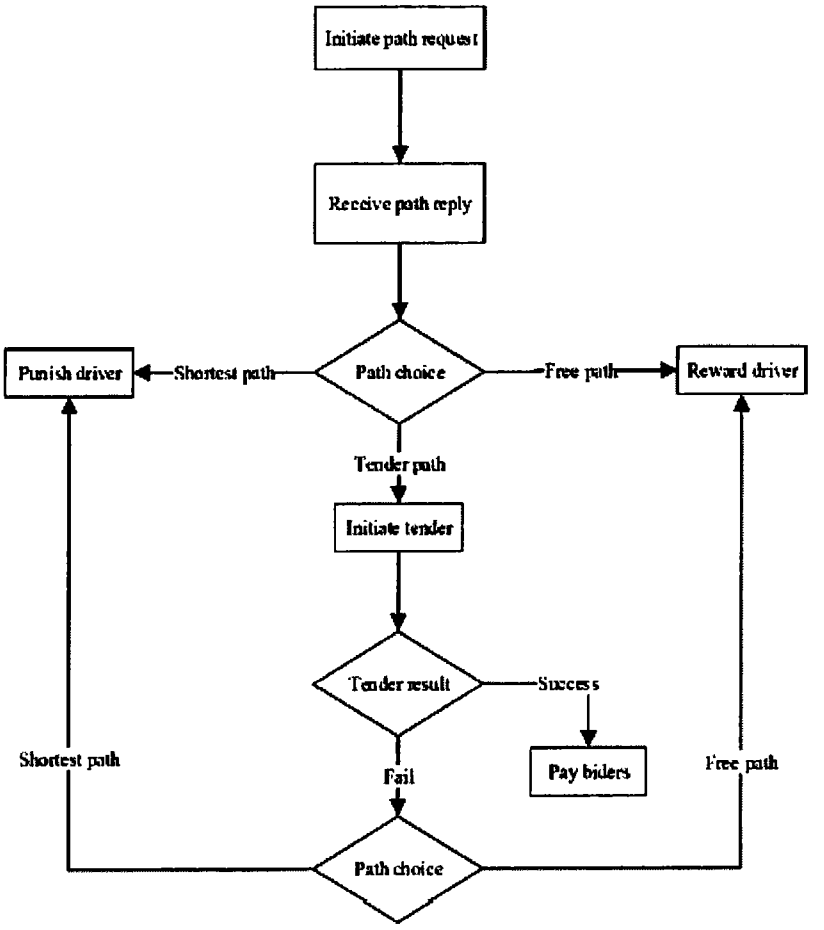


Figure: 6.2: Path Selection Mechanism

6.2.4 Path Selection Mechanism

In order to select best path, the RSU recommends a set of roadways, these roadways are reserved and called critical routes. While in case of free routes, the free routes will significantly reduce the traveling delay on roadways. In the mentioned case, vehicular nodes are agreed to payment for using these free routes. RSU tenders for traffic on these free route sections. The bidding process follow the hidden envelope mechanism for optimal price selection, in which the vehicle broadcasts a message with a key section ID to show its willingness to use free routes for payment of T-credit coins. The bid request message also contains the cut-off date for bidding. After receiving the bid quotation, if the vehicle (driver) confirms the quotation, it sends a route update to the server, and the successful bidder obtains the specific T-Credit coins. The detailed steps of the route reservation and bidding process are shown in Figure 6.2.

6.3 Reward and Punishment Scheme

The proposed work mainly focused on the encouragement of nodes/vehicles in VANET to vigorously contribute in message forwarding, vehicular nodes monitoring and misbehavior reporting. These factors are considered to be the main responsibilities of each node to attain an effective VANET model. We believe that this encouragement can be done effectively when the nodes work together as a team (a cluster in VANET). In addition, cluster based message forwarding approach can act better in sending and receiving of data and monitor the behavior of participating nodes. Therefore, we proposed a trust-reputation scheme for cluster-based forwarding, in which incentives or payments are provided to nodes to incentivize the smooth operation of the above functions. The payment of the proposed mechanism is carried out in three different phases, namely (i) participation in elections process, (ii) data forwarding phase, and (iii) monitoring and evaluation of other nodes. These stages will be clarified further in the following subsections.

6.3.1 Reward for Participation in Election

We implemented a weight-based clustering approach to select Cluster Head (CH) for every cluster in VANET. The node that shows attributes such as more neighbors' nodes, positional relativity, average positional speed, and average speed of the vehicular node

produces the low weightage and becomes CH. The second lowest weightage node will be selected as Auxiliary Cluster Head (ACH).

The objectives of ACH are to keep the stability of the cluster by taking the responsibilities when the CH is vanished. For this reason, the CH soon after the election immediately uses its own MAC ID to generate a unique cluster-ID. This id is maintained as a cluster-ID by succeeding ACH till both CH and ACH are vanished. However, if two nodes have the same weight, all nodes will wait for a define time interval to resend their weightages. Each vehicle A compares the RSS mode with its neighbors similarly $N1; N2...:Nk$, $\forall Ni; Nj \in N(A)$.

Trust Calculation: In our context, the frame of discernment Ω contains two elements, namely $\Omega = \{+T, -T\}$. Where +T indicates that the vehicle is credible. -T indicates that the vehicle is not credible. Hence, there are three propositions: proposition S = {+T} representing that the evaluated vehicle is credible; proposition S' = {-T} representing that the evaluated vehicle is not credible; proposition U = {+T,-T} representing that the evaluated vehicle is either credible or malicious.

Assume that the reputation value of V_i is R_e. If vehicle V_j states that vehicle V_i is credible, then the BPA of vehicle

$$m_1(V_i) = R_e; \quad m_1(V_i) = 0; \quad m_1(V_i) = 1 - R_e \tag{6.1}$$

If vehicle V_j states that vehicle V_i is not credible, then the BPA of vehicle are:

$$M_2(V_i) = 0; \quad m_2(V_i) = R_e; \quad m_2(V_i) = 1 - R_e \tag{6.2}$$

If the TA receives k trust reports on vehicle V_j, the credibility of the vehicle V_j is:

$$C_r(V_i) = m(V_i) = \sum_{j=1}^{k} mj(V) \tag{6.3}$$

Throughout the thesis, we assume that if $C_r(V_i) > 0.5$, the evaluated vehicle is credible, while if $C_r(V_i) > 0.5$, the evaluated vehicle is malicious. In the second case, the TA will update the vehicle's reputation.

In general, proposed model consists of n participants, where each participant n_1; $n_2 \ldots : n_k$, n_i; $n_j \in N(A)$ and Ω has some private information, known as participation ratio. A participant n_i can choose any strategy U to input in the mechanism. Based on the inputs of all participants, the mechanism calculates a specific payment vector P_1: P_2 ...P_n for each participant and a global output Z_1: Z_2... Z_n. From the output, the preference of each participant is calculated as a cost function With this information, the utility of a participant n_j can be calculated as $\sum_{j=1}^{k} Pn(Zn)$. We use this reward and punishment scheme with a minor modification to contract with diverse VANET features. For example, previous VANET reward model used the RSS approach treated the energy levels of nodes and imposed truth telling features when revealing available energy. However, RSS value or energy level is not the primary concerns of VANET. We take in to account the reputation weightage scores as private information for modeling an effective and robust incentive scheme for VANET, the incentive mechanism can be calculated based on the trust reports and reputation score of each vehicle and made public for participation in elections. In addition, based on the principle of reward and punishment, each node is assigned a real number called reputation score R_S. After each election, this R_S will increase to a certain range based on the authenticity of selfish behavior of the participating node.

Algorithm 6.1 Reward for Participation in Election Process

1: For each Node i

2: Set U = {+T,-T}

3: V_i compute and broadcast Ω.

4: $V_i \in N(A)$

5: If $Td < \eth$ for V_i

6: $C_r(V_i) > 0.5$ and $\sum_{n=1}^{k} Vi(U) + ITx$

7: invokes incentive awarding for V_i

8: V_i exchanges the Incentive Transaction IT_x with destination node.

8: V_i sets $IT_x = IT_x + 2$

10: end

6.3.2 Reward for Message Forwarding

In the proposed approach, we only confine the CH and ACH to act as intermediate forwarding nodes for sending data packets. However, if the operation performed does not benefit the forwarding node, the forwarding node may avoid taking such responsibility. Such unusual behavior in VANET will have negative impacts on cluster constancy, the ratio of cluster dis connectivity, and increase in end-to-end delay and packet loss rate. Therefore, in order to encourage forwarding nodes to complete their work in a responsible way, we provide rewards/compensation for each forwarder. In order to effectively grant these payments, we use other nodes as watchdogs to observe the performance of the forwarding nodes. According to their judgment, the relay node is judged as cooperative or uncooperative, and pays it accordingly.

In this section, we discussed incentive-based forwarding mechanism to pay reward to vehicle for successful message delivery across the network. In case, if *RSU* needs to send a message m to V_i through store-carry-forward mechanism with the assistance of MS. Then *RSU* demands V_i to carry out a message m to *RSU*, the system initiate an incentive transaction IT_x for *RSU*. If V_i successfully finishes the message forwarding process for *RSU* then incentive transaction IT_x is credited to the system network. The incentive transaction IT_x can be cashed by *RSU* using Encashment Signature (E-Sig) transaction.

In case, if V_i does not send the message m to *RSU*, *RSU* will lose its incentive. Once IT_x is credited to the system, the *RSU*'s input value of IT_x is termed as consumed in the incentive scheme. To handle with this condition, we set time-stamp T_s condition locked with E-Sig for *RSU* to draw the incentive from IT_x. This scheme is suitable in case where V_i deliberately not to forward the message earlier than the time-stamp lock condition expires.

Algorithm 6.2 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 6.2 Reward for Message Forwarding

1: For each Node i

2: Set U = {+T,-T}

3: V_i compute and broadcast Ω.

4: $V_i \in N(A)$

5: If $Td < \eth$ for V_i

6: $C_r(V_i) > 0.5$ and $\sum_{n=1}^{k} Vi(U) + ITx$

7: invokes incentive awarding for V_i

8: V_i exchanges the Incentive Transaction IT_x with destination node.

8: V_i sets $IT_x = IT_x + 2$

10: end

6.4 Results and Discussion

The incentives payments to cooperative nodes are done through proposed RIPA model. Node-participation in the election process is rewarded for showing cooperation in the network, and can become CH and ACH during election process. Nodes that have selfish behavior and have not shown the required responsibilities will receive negative payments as rewards. When a node repeatedly exhibits selfish behavior, it will be penalized in the procedure of expelling the network.

6.4.1 Resources Utilization

We consider the problem of resources utilization in VANET where the selfish nodes attempts that his resources cannot be used for other communication. Selfishness is further separated into two major types; Node centric selfishness and data centric selfishness. In case where vehicle attempt that his resources cannot be utilized by others, this type of selfishness is called node centric selfishness. While in data centric selfishness vehicular node propagate false and bogus event driven messages (congestion) to change the direction and normal flow of traffic.

CH and ACH can decide whether to use or not to use node resources for forwarding message across the network for minimizing TTL values, while the RSU can assign system and computing resources to other nodes. We offer a certain credits coins to participating nodes which serves as a volunteer forwarder for the created message forwarding of other

nodes. Our data analysis in the following tables and figures show that the central allocation mechanism provide an efficient and robust approximation for resources utilization and can improve transmission delay of data packets. Resources utilization parameters and values are depicted in Table 6.1.

Table 6.1: Resources Utilization Values

Resources Utilization				
	Minimum	**Average**	**Maximum**	**Last**
Node Util.	0.00 %	0.38 %	3.96 %	0.55 %
Channel Util.	0.00 %	0.00 %	0.04 %	0.00 %
System Util.	0.00 %	0.12 %	0.81 %	0.43 %
Battery Util.	0.00 %	0.01 %	0.09 %	0.00 %
No. of Nodes	197.84	207.35	222.11	221.00

Figs. 6.3-6.6, shows the resources utilization graph for define parameter like Node Utilization, Channel utilization, System Utilization, and Battery Utilization for participating vehicles on the roads. Fig. 6.3 depicted the minimum resources utilization in message forwarding in the network. As shown in graph, Node Utilization is 0.05%, channel Utilization is 0.00%, System Utilization is 0.02%, and Battery Utilization is 0.001233 %. Hence, we can infer that a specific node at point 197.84 showing selfish behavior and the resource Utilization value for this specific vehicle is 0.00%.

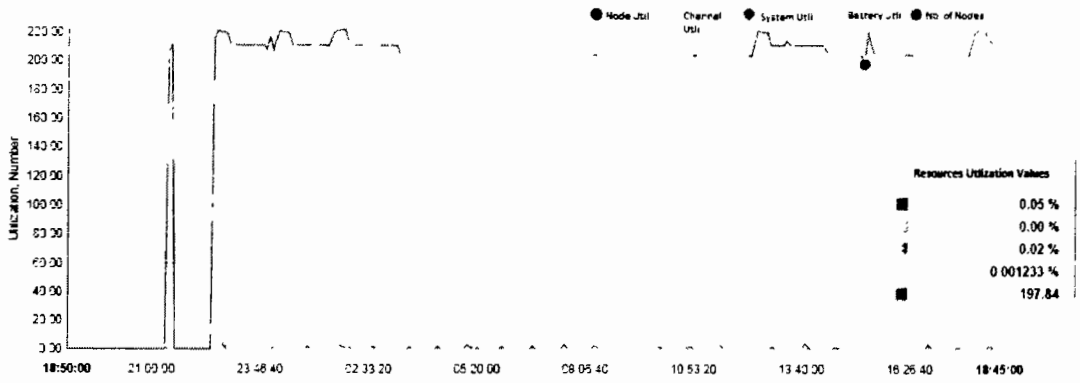


Figure: 6.3. Resource Utilization Value at Node Point 197.84.

Fig. 6.4 depicted the average resources utilization in message forwarding in the network. As shown in graph, Node Utilization is 1.03%, channel Utilization is 0.00%, System Utilization is 0.48%, and Battery Utilization is 0.00 %. It is very important to note that Node utilization and System Utilization are the two major effective impact factors during messages forwarding. Therefore, a slight increase in the values of these parameters at point 207.56 will be termed as average utilization ratio in the network. In VANET, Battery utilization and channel capacity utilization does not affect the system performance as vehicular nodes are not confined to battery and channel limitations.

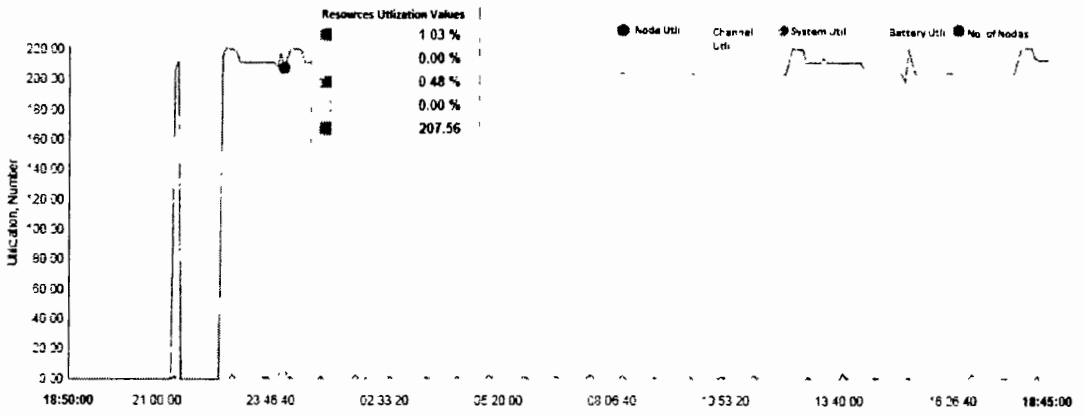


Figure: 6.4. Resource Utilization Value at Node Point 207.56.

Fig. 6.5 illustrated the maximum resources utilization in message forwarding in the network. As shown in graph, Node Utilization is 3.96%, channel Utilization is 0.04%, System Utilization is 0.81%, and Battery Utilization is 0.09%. It is very obvious from Fig. 6.5 that all factors of Node utilization, Channel Utilization, System Utilization, and Battery Utilization shows exponential increase in the values of these parameters at point 222.11 will be termed as maximum utilization ratio in the network. The depicted Graphs show that the resources are fully utilized in the message forwarding mechanism of the proposed scheme. The ratio of selfish and misbehaving vehicular nodes at this point can be greatly reduced by the cooperative nodes participation.

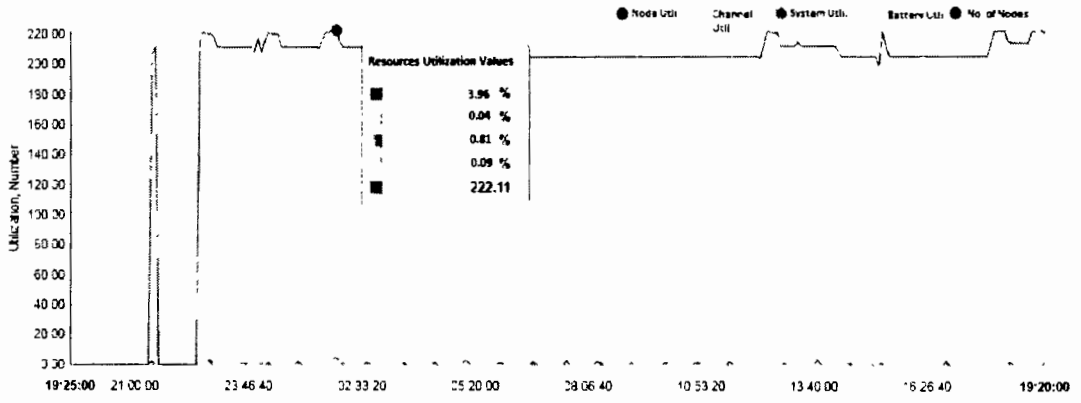


Figure: 6.5. Resource Utilization Value at Node Point 222.11.

Fig. 6.6 depicted the last resources utilization in message forwarding in the network. As shown in figure, Node Utilization is 0.35%, channel Utilization is 0.00%, System Utilization is 0.16%, and Battery Utilization is 0.00 %. As discussed earlier that Node utilization and System Utilization are the two major effective impact factors during messages forwarding. Therefore, a slight increase in the values of these parameters at point 221.00 will be termed as last utilization ratio of the network.

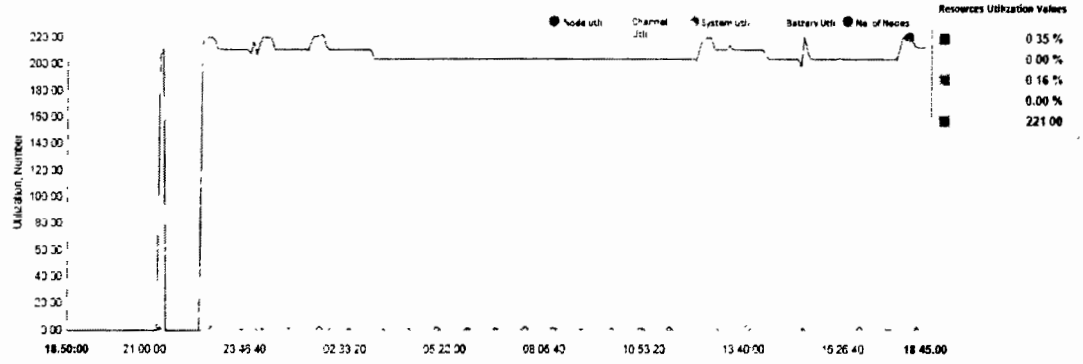


Figure: 6.6. Resource Utilization Value at Node Point 221.00.

6.4.2 Experimental Results

Reputation of a node can be determined by the cooperative and misbehavior nature of the participating vehicular node. Figure 6.7 shows the variation of node reputation in different

time intervals during selection of CH and ACH. The experimental results show that misbehaving nodes in VANET decrease the node reputation during selection process.

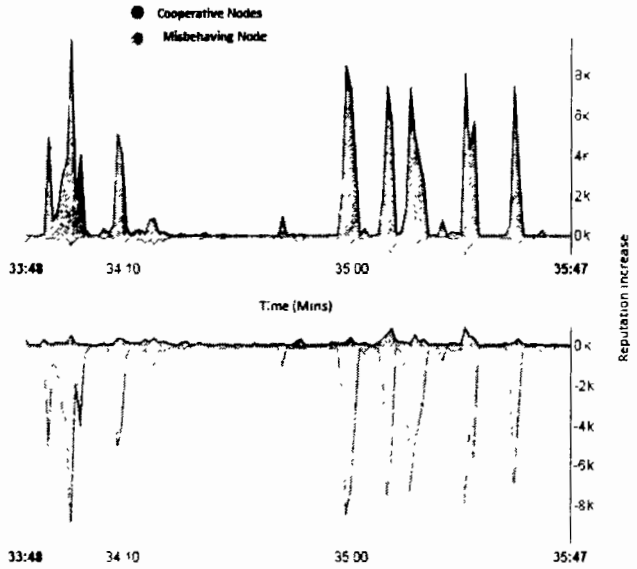


Figure: 6.7. Reputation Increase over Different Time Intervals

In Fig. 6.8, the effects of misbehavior vehicular nodes on the data packets forwarded are examined in the circumstance where no motivating force collaboration is carried out. In the simulating environment, an acting misbehavior node will just sent its self-made messages and refused to forward those made by other vehicular nodes. Fig. 6.8 portrayed the effect of the acting misbehavior node on Data Packets Forwarded or Packet Delivery Ratio (PDR) of the proposed Reputation-based Incentive and Punishment Approach (RIPA) with existing [211] Payment and Punishment Scheme (PPS). The decline line in Fig. 6.8 shows the decline inclination of the PDR or Data Packets Forwarded as the extent of misbehaving nodes increased.

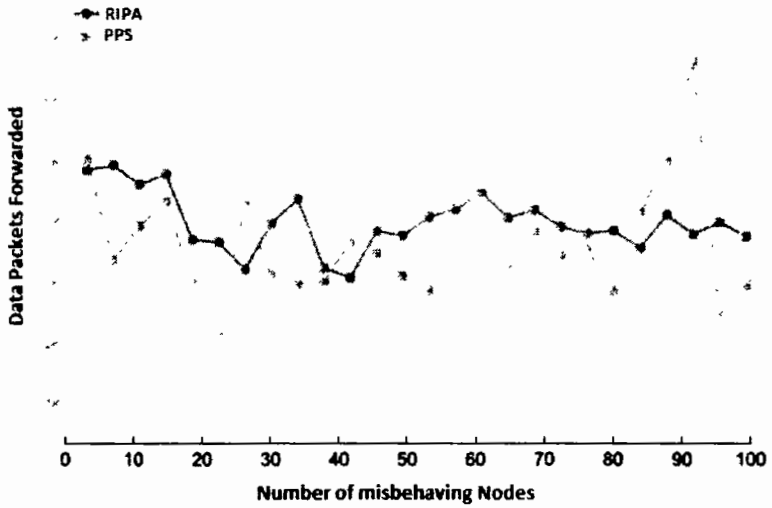


Figure: 6.8. Effect of Number of Misbehaving Nodes on Data Packet Forwarding Rate

Fig. 6.9 illustrated the credit coins rewarded incentives of the suggested scheme. It is very clear from Fig.6.9 that increase in the number of forwarded packets, the accumulated compensated credit coins will escalated intensely with the high proportion of forwarded packets at the destination point. As shown in graph that in our proposed RIPA approach, the aggregated rewarded credits are greater than that of PPS scheme. Moreover, the average forwarded data packet in the proposed RIPA approach is much higher than that of the existing PPS approach.

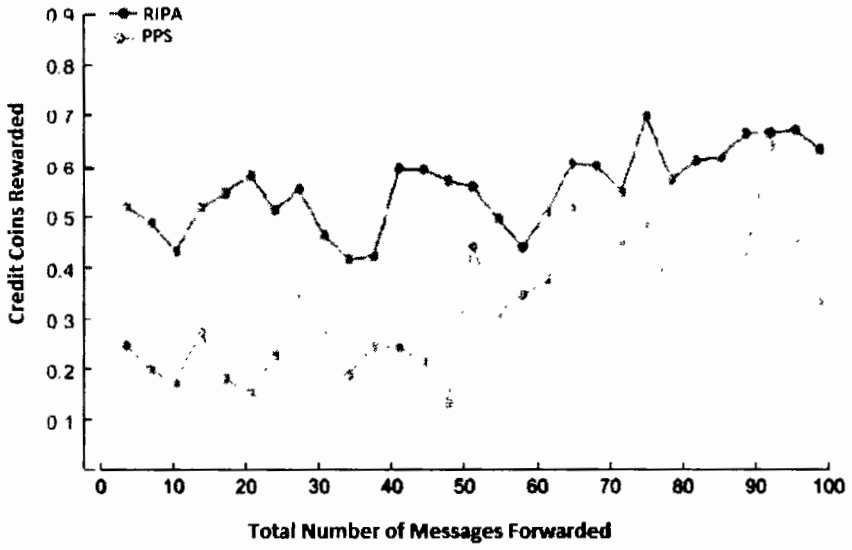


Figure: 6.9. Incentive-Driven Messages Forwarding

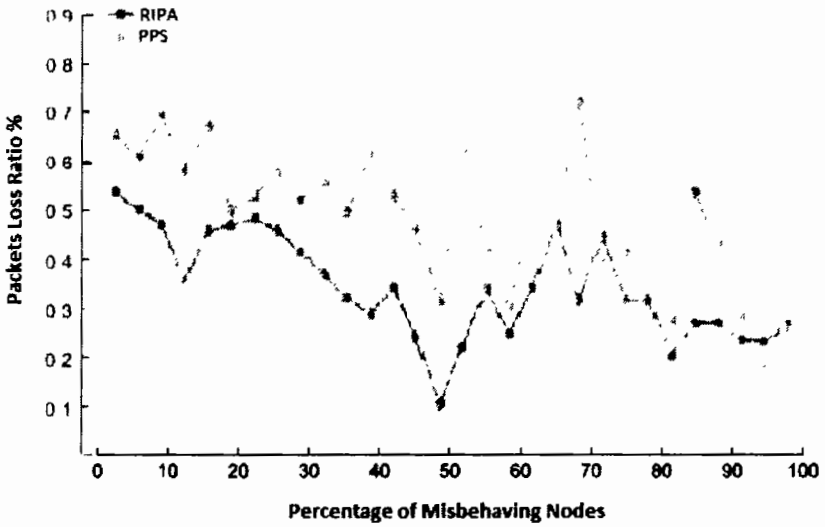


Figure: 6.10. Effects of Misbehaving Nodes on Packet Loss Ratio

Fig. 6.10 depicted the deterioration inclination of the Packet Loss Ratio as the proportion of the misbehaving nodes increases. The graph represents the decline rate of the Packet Loss Ratio when a large number of misbehaving nodes exist in VANET. In such a case when the proportion of misbehaving vehicles increases, the transmission delay will also raise exponentially.

Since percentage of misbehaving and cooperative influence average reputations, the impact of cooperative node behavior stimulate average reputation score. Figure 6.11 shows the overall increase in reputation score throughout the experimental process, and different cooperative nodes in the election process. Obviously, when the number of cooperative nodes increases, the average reputation score of the participating nodes also increases.

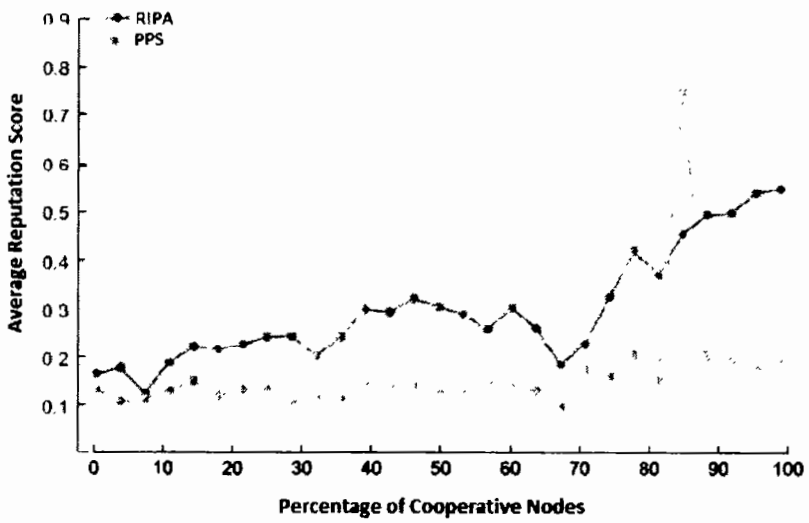


Figure: 6.11. Impact of Cooperative-based Communication and Reputation Score

Fig. 6.12 defines the impact of false positive ratio with varying number of CH and ACH. False positive rate in the RIPA scheme can be described as misbehaving nodes claiming to be honest or cooperative nodes in the reputation calculation phase. It is very obvious from the Fig. 6.12, that the false positive ratio of both RIPA and PPS schemes decline with increased number of CH and ACH. However, dealing with Quality of Services (QoS), the lower number of Cluster Heads will lead to controversial assessment of the reputation calculation mechanism. Therefore, the proposed model involves additional number of CH for providing an accurate assessment. Figure 6.12 describes the combined assessment and suggested that at least two cooperative nodes with different behavior factors in RIPA can be sufficient for deriving accurate assessments. While in some rare cases where more than nodes have the same reputation scores, a third CH will be deputed to provide assessments

report. Hence, we can determine that more than two CH are necessary for providing accurate assessments, and false positives ratio will be negligible in such cases.

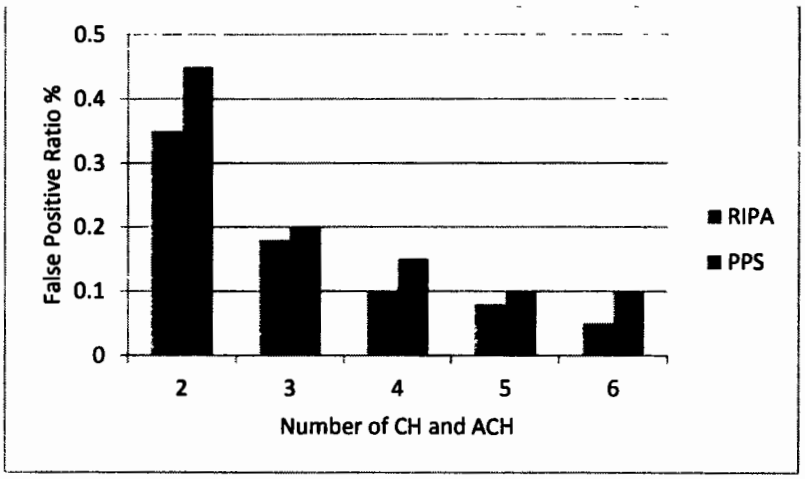


Figure: 6.12. Percentage of False Positive Rate with varying Number of CH and ACH

As payment to the forwarder node is based on CH and ACH assessments, RIPA approach follows a robust mechanism for the payment transaction based on detection ratio of the misbehaving nodes.

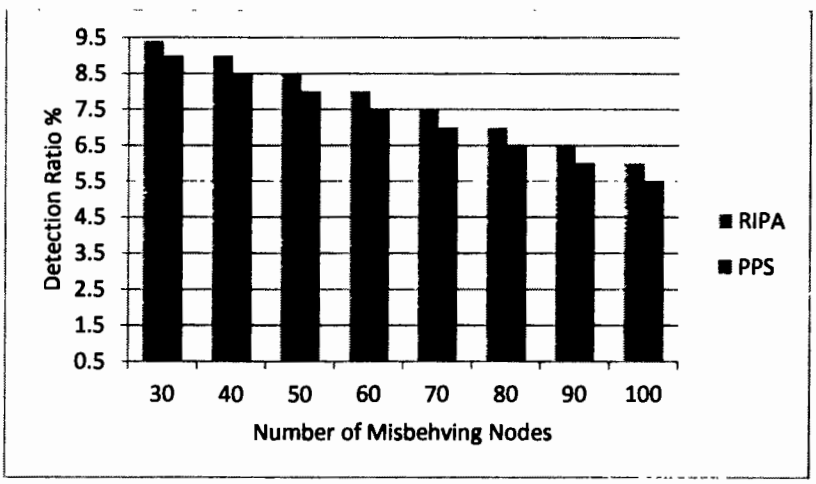


Figure: 6.13. Detection ratio of Misbehaving Nodes

Fig. 6.13 depicted the detection ratio of the proposed and existing schemes. It can be noticed that when detecting misbehaving nodes, the performance of RIPA is better than

QoS threshold, the proposed shows that the detection ratio of all misbehaving nodes is round about 95%. This is because of the indication that various CH will be preserved different importance factors for reputation calculations.

6.5. Chapter Summary

In this chapter, we discussed the integrated trust-based incentive driven scheme to motivate participating nodes in dissemination of messages across VANET. The cooperation-based implementation techniques of wireless ad hoc network are divided into two categories: (a) Shaping trust through reputation scheme and (b) credit-based approach. Apart from predictable reputation-based credit approaches, firstly, the proposed research work plots a Path Reservation Policy for efficient and secure routing across the network, secondly, path selection mechanism is followed in order to select the best and free path for messages exchange. At last, the reward and punishment strategies implemented to incentivize the cooperative nodes participated in election of CH and ACH. To enhance the effective messages forwarding strategies, the proposed scheme adopted a comprehensive Credit-Coin based reward for relay nodes. The Experimental results mainly focused on major performance factors i.e. Resources Utilization, Reputation Increase, Lowering Packet Loss Ratio, Effective Message Forwarding using Credit–Coin Approach, Reduction in FPR, and enhancing Detection ratio of Misbehaving Nodes. Simulation results show the proposed scheme achieved significant improvement in the define performance metrics.

7. Conclusion and Future Work

In this research work, we proposed a Collaborative-trust based malicious detection scheme to observe fake data dissemination and data non-forwarding techniques in VANET. To tackle fake data detection, a trust model for data integration is proposed based on collaborative Approach. The proposed model analyzed communication features which consist of emergency event information such as event reports and location verification. For message non-forwarding detection, we proposed a collaborative-trust scheme converging on the behavior features of vehicles in context with data propagation. Every vehicular node uses collaborative-trust approach and SVM kernel based classification module to determine whether a specific vehicular node is trustworthy for sending the trust evaluation reports to the Trust Authority. Trust Authority uses CBMA module to integrate several trust evaluation reports for a particular vehicle. We proposed Gaussian kernel function for SVM classification which best suits our Collaborative-trust scheme. Experimental results show that collaborative-trust scheme has considerably high malicious data detection ratio and cannot be influenced by the vehicular reputation scores and proportion of misbehaving vehicular nodes in VANET. After comparing with CoCoWa, MV, DST, and BI, our collaborative-trust scheme is more appropriate and robust; in context of the detection ratio of malicious node our proposed scheme shows better results. The proposed scheme shown much higher TPR ratio with different network primitives like number of training samples, average reputation score of malicious vehicles and number of messages exchanged. However, apart from detection of maliciousness there are some uncertain situations like Sybil and DoS attacks, where the proposed mechanism could be extended to avoid the unseen situations. In addition, it is very important to note down that a lot of calculations can be made by TA to get and integrate multiple trust reports.

In the proposed research work, we also proposed cooperative-based trust (CBT) scheme integrating with comprehensive credit rewarded scheme using certified public key for VANET. Vehicular reputation can be assessed using collaborative trust evaluation

approach; trusted route selection mechanism is adopted to ensure reliable communication pathways. The proposed Reputation-driven Incentive and Punishment (RIPA) scheme employed incentive driven message forwarding approach to motivate vehicular node for their honest cooperation in the network. In order to avoid node from misbehaving, a stimulus approach is adopted where vehicles can get rewards for their volunteer efforts and positive cooperation with other vehicle on the network In proposed scheme, fairness and security can be guaranteed by using E-Sig 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 secure communication, we also employed Incentive Transaction Lock and unlock scripts integrated with time-stamp locked condition to deal with security aspects of the communication. Furthermore, in contrast with the existing schemes, our proposed cooperative based scheme shown better outcome for transmission delay, Packet Delivery Ratio (PDR), Effectiveness of credit rewards over network performance, Computation overhead, and Participation ratio of honest nodes.

In future work, for ensuring efficient and robust messages forwarding the resources utilization mechanism should be based on trust-credit integration for VANET. As we know that there is also a confined contact (short-term connectivity) between the vehicles in ad-hoc networks. Hence, the connectivity and trust-based credit model to be further enhanced for meaningful communication in VANTs. As the designing of the reputation calculation module is a significant and complicated matter, we still need to focus extensive research to tackle this issue in our future work.

Biblography

[1] Dedicated Short Range Communication working group, "*Dedicated Short Range Communications*".http://grouper.ieee.org/groups/scc32/dsrc/index.html, outline, 2015.

[2] S. Grafling, P. Mahonen, J. Riihijarvi, "Performance evaluation of IEEE 1609 WAVE and IEEE 802.11p for vehicular communications," in Proc. *Second Inter-national Conference on Ubiquitous and Future Networks (ICUFN),* 2010, IEEE, pp. 344–348.

[3] S. Eichler, "Performance evaluation of the IEEE 802.11 p WAVE communication standard, in *Proc 66th Vehicular Technology Conference, 2007. VTC-2007,* IEEE, pp.2199–2203.

[4] A . Dua, N. Kumar, S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Veh. Commun.*, Vol. 1(1), pp. 33–52, 2014.

[5] F. Li, Y. Wang, "Routing in vehicular ad hoc networks: a survey," *IEEE Veh. Technol. Mag.*, Vol.2 No.2, pp. 12-22, 2007.

[6] A. Gainaru, C. Dobre, V. Cristea, "A realistic mobility model based on social networks for the simulation of VANETs," in *Proc. IEEE 69th Vehicular Technology Conference, 2009, VTC* IEEE, 2009, pp.1–5.

[7] J. Sun, Y. Fang, "Defense against misbehavior in anonymous vehicular ad hoc networks," *Ad Hoc Netw.*, Vol. 7(8), pp. 1515–1525, 2009.

[8] J.M. Pozo, O. Trullols, J.M. Barceló, J.G. Vidal, "A cooperative ARQ for delay-tolerant vehicular networks," in *Proc. 28th International Conference on Distributed Computing Systems Workshops, ICDCS'08*, IEEE, 2008, pp.192–197.

[9] L. Aparecido, "Data dissemination in vehicular networks: challenges, solutions, and future perspectives," in *Proc. 7th International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2015, pp.1–5.

[10] S. Yousefi, M.S. Mousavi, M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," in *Proc. 6th International Conference on ITS Telecom-munications Proceedings, IEEE,2006,* pp.761–766.

[11] B. Paul, M. Ibrahim, M. Bikas, A. Naser, "Vanet routing protocols: pros and cons," *International journal of computer applications*, Vol. 20, No. 3, pp.1-12, 2011.

[12] J. Park, Y.S. Jeong, S. Park, H.C. Chen, "Embedded and Multimedia Computing Technology and Service," *Lecture Notes in Electrical Engineering,* Springer, Vol.181, 2012.

[13] R. van der Heijden, S. Dietzel, F. Kargl, "Misbehavior detection in vehicular ad-hoc networks," in *Proc. 1st GI/ITG Inter-Vehicle Communication, Institute of Distributed Systems*, 2013, pp. 102-114.

[14] A. Daeinabi, A. Ghaffarpour, "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks," *Multimed Tools Appl.* Vol. 1(78), pp. 325–338, 2013.

[15] P. Sangulagi, M. Sarsamba, V. Katgi, "Recognition and Elimination of Malicious Nodes in Vehicular Ad Hoc Networks (VANET's)," *Indian Journal of Computer Science and Engineering (IJCSE).* Vol.2 (4), pp 16-22, 2013.

[16] N. Haddadou, A. Rachidi. Y.Ghamri-Doudane, "Trust And Exclusion In Vehicular Ad Hoc Network : An Economic Incentive Model Based Approach," *IEEE Transaction.* IEEE, pp 13-18, 2013.

[17] N. Haddadou, A. Rachidi. Y.Ghamri, "A Job Market Signaling Approach Scheme for Incentive and Trust Management in Vehicular Ad Hoc Network," *IEEE Transactions on Vehicular Technology*, Vol. 64, NO. 8, IEEE, pp 3657-3674, 2015.

[18] Z. Huang, A. Marcos Cavenaghi, M. Stojmenovic, "A social network approach to trust management in VANETs," *Peer-to-Peer Netw. Appl.*, Springer, Vol.7, pp 229-242, 2014.

[19] U Khan, S Agrawal, S Silakari, "A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks," *Information Systems Design and Intelligent Applications.*, Springer, Vol. 15(2), pp. 45-56, 2015.

[20] R. W van der Heijden, S. Dietzel, T. Leinmuller, F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems,".1610.06810 Springer, *2016.*

[21] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari and A. Tyagi, "Vehicular Security through Reputation and Plausibility Checks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 384-394, 2014.

[22] S. Ruj, M.A Cavenaghi, Z. Huang, A. Nayak, "Data-Centric Misbehavior Detection in VANETs," in Proc. *Vehicular Technology Conference (VTC Fall), 2011, IEEE.* IEEE, pp. 1–5.

[23] Y. Hua Ho, C. Han Lin, L. Jyh Chen, "On-demand Misbehavior Detection for Vehicular Ad Hoc Network," *International Journal of Distributed Sensor Networks* (IJDSN)., Vol. 12(10). pp. 1-14 , 2016.

[24] W. Liang, Z. Li, H. Zhang, S. Wang, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges and Trends," *International Journal of Distributed Sensor Networks IJDSN.*, Vol 11. No. 8, pp. 745303, 2015.

[25] M. Arshad, Z. Ullah, H. Criuck shank, Y. Cao, "A survey of local/cooperative based malicious information detection techniques in VANETs," *Journal on Wireless Communications and Networking,* Vol. 62(18*)*, pp-1-24, 2018.

[26] J.Molina-Gil, P. Caballero-Gil, C. Caballero-Gil, "Countermeasures to prevent misbehaviour in VANETs," *J. UCS.,* Vol. 18(6), pp. 857–873, 2012.

[27] E. Hernandez-Orallo, D. Olmos, C. Cano, T. Calafate, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," *IEEE Transactions on Mobile Computing.,* Vol. 14, No. 6. IEEE. pp. 1162-1175, 2015.

[28] L. ChauHua, M. Hossein, Y. PorLip, "Social networking-based cooperation mechanisms in vehicular ad-hoc network-a survey," *Vehicular Communications.,* Vol. 10 (17), pp 57-73, 2017.

[29] T.J Kim, A. Studer, R. Dubey, X. Zhang, A. Perrig, F. Bai, B. Bellur, A. Iyer, "VANET alert endorsement using multisource filters ACM," in Proc. *Seventh ACM International Workshop on VehiculArInterNETworking.*, 2010, pp. 51–60.

[30] T . Zaidi, S. Giri, S. Chaurasia, "Malicious Node Detection through AODV in VANET," *International Journal of Ad hoc, Sensor &Ubiquitous Computing.*, Vol.9, No. 2, pp. 33-43, 2018.

[31] A. Vulimiri, A. Gupta, P. Roy, S. Muthaiah, A. Kherani,. "Application of secondary information for misbehavior detection in VANETs," In Proc. *International Conference on Research in Networking.*, 2010, pp. 385–396.

[32] K. Sha, S. Wang, W. Shi, "*RD*4: Role-differentiated cooperative deceptive data detection and filtering in vanets," *IEEE Trans. Veh. Technol.* Vol. 59(3), pp. 1183–1190, 2010.

[33] J. Rezgui, S. Cherkaoui, "Detecting faulty and malicious vehicles using rule-based communications data mining," in Proc. *36thIEEE Conference Local Computer Networks (LCN),*2011, pp. 827–834.

[34] D. Huang, S. Williams, S. Shere, "Cheater detection in vehicular networks," in Proc. *IEEE 11th Trust, Security and Privacy in Computing and Communications (TrustCom), International Conference.,* 2012, pp. 193–200.

[35] K. Zaidi, M. Milojevic, V. Rakocevic, M. Rajarajan, "Data-centric rogue node detection in vanets," in Proc. *13th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2014, pp. 398–405.

[36] K. Zaidi, M. Milojevic, V. Rakocevic, A. Nallanathan, M. Rajarajan, "Host-based intrusion detection for vanets: a statistical approach to rogue node detection," *IEEE Trans. Veh. Technol.*,Vol. 65(8), pp. 6703–6714, 2019.

[37] R.W Van der Heijden, F. Kargl, OM. Abu-Sharkh, A. Al-Momani, "Enhanced position verification for vanets using subjective logic," In Proc. *IEEE Vehicular Technology Conference*, 2016, Universitat Ulm.

[38] SK. Harit, G. Singh, N. Tyagi, " Fox-hole model fordata-centric misbehaviour detection in vanets," In Proc. *Third International Conference* on *Computer and Communication Technology(ICCCT)*, IEEE, 2012, pp. 271–277.

[39] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs. in Proc. *1st ACM International Workshop on Vehicular Ad Hoc Networks*. ACM, 2004, pp. 29–37.

[40] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, JP. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Selected Areas Commun*. Vol. 25(8) , 2007.

[41] A. Rivero Garcia, I. Santos Gonzalez, P. Caballero Gil, C. Caballero Gil, "Vanet event verification based on user trust," in Proc. *24th Euro micro International Conference On Parallel, Distributed, and Network-Based Processing (PDP)*, IEEE, 2016, pp. 313–316.

[42] B. Płaczek, M. Bernas, "Detection of malicious data in vehicular ad hoc networks for traffic signal control applications," in Proc. *International Conference on Computer Networks*.. Springer, 2017, pp. 72–82.

[43] H. Al Falasi, N. Mohamed, H. El-Syed, "Similarity based trust management system: data validation scheme," *Hybrid Intelligent Systems*. Springer, pp. 141–153,2016.

[44] N. Fan, Q. Wu, "Trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Networks,* Elsevier, 2018, pp 1-13.

[45] H . Hasrouny, A. Ellatif Samhat, C. Bassilc, A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications.*, Elsevier, Vol. 7(2017), pp. 7-20, 2017.

[46] Z. Soltani, K. Mizanian "Misbehavior Node Detection in Vehicular ad-hoc Networks: A survey, With Special Emphasis on Multihop Broadcast Protocols," *Researcher* Vol. 9(1), pp. 41-46, 2017.

[47] C.H Kim, I.H Bae, "A misbehavior-based reputation management system for VANETs," *Embedded and Multimedia Computing Technology and Service.*, Springer, pp. 441–450, 2012.

[48] A. Ahmed, kamalrunizam, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," *Frontiers of Computer Science.*, Springer, Vol. 9(2), pp.280–296, 2015.

[49] Santos J., L.M., Moreira, E. "|An evaluation of reputation with regard to the opportunistic forwarding of messages in VANETs,"| *J Wireless Com Network*, Vol. 204, 2019.

[50] K. Govindan, P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Commun. Surv. Tutorials.* Vol. 14(2), pp. 279–298 , 2012.

[51] R. van der Heijden, S. Dietzel, F. Kargl, "Misbehavior detection in vehicular ad-hoc networks," in Proc. *1st Fachgesprach Inter-Vehicle Communication (FG-IVC 2013*, pp. 201-223.

[52] T. Lu, S. Chang, and W. Li, "Fog computing enabling geographic routing for urban area vehicular network," *Peer Peer Netw. Appl.*, vol. 11, no. 4, pp. 749-755, 2018.

[53] A. Ltifi, A. Zouinkhi, M. Bouhlel, "An Alert Endorsement through Cooperative Trust Management for VANET," *International Journal of Computer Science and Information Security (IJCSIS).* Vol. 10. No.4, 2012.

[54] N. Bismeyer, S. Mauthofer, KM. Bayarou, F. Kargl, "Assessment of node trustworthiness in vanets using data plausibility checks with particle filters," In Proc. *Vehicular Networking Conference (VNC),* IEEE, 2012, pp. 78–85.

[55] R. Abassi, C. Ben, and D. Sauveron, "TSME: a trust-based security scheme for message exchange in vehicular Ad hoc networks," *Hum. Cent. Comput. Inf. Sci.* Vol. 10, No. 43, 2020.

[56] Z. Cao, J. Kong, U. Lee, M. Gerla, Z. Chen, "Proof-of-relevance: filtering false data via authentic consensus in vehicle ad-hoc networks," In Proc. *INFOCOM Workshops* IEEE, 2008, pp. 1–6.

[57] F. Dotzer, L. Fischer, P. Magiera, "A. Vars: A vehicle ad-hoc network reputation system," in Proc. *Sixth IEEE International Symposium World of Wireless Mobile and Multimedia Networks., WoWMoM* .IEEE, 2005, pp. 454–456.

[58] N. W Lo, H.C Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP J. Wirel. Commun. Netw.*, Vol. 1, pp. 25-48, 2009.

[59] Q. Ding, X. Li, M. Jiang, X. Zhou, "Reputation-based trust model in vehicular ad hoc networks," in Proc. *International Conference on Wireless Communications and Signal Processing (WCSP),* IEEE, 2010, pp. 1–6.

[60] Z. Huang, S. Ruj, M. Cavenaghi, A. Nayak, "Limitations of trust management schemes in VANET and countermeasures," In Proc. *22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC),* IEEE, 2011, pp. 1228–1232

[61] D. Aniket, "Review of Effective Trust Management Systems in VANET Environments," *International Journal of Grid and Distributed Computing*, Vol. 14. Pp. 1771-1780. 2021.

[62] Z. Abdulkader, A. Abdullah, M. Abdullah, Z. Zukarnain, "Vehicular ad hoc networks and security issues: survey," *Modern Appl. Sci.* Vol. 11(5), No. 30, 2017.

[63] D. Zhang, F. Yu, Z. Wei, A. Boukerche, "Software-defined vehicular ad hoc networks with trust management," In Proc. *6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*. ACM, 2016, pp. 41–49.

[64] A. Alkalbani, A. Tap, T. Mantoro, "Energy consumption evaluation in trust and reputation models for wireless sensor networks," in Proc. *5th International Conference on Information and Communication Technology for the Muslim World (ICT4M),* IEEE, 2013, pp. 1–6.

[65] X. Yao, X. Zhang, H. Ning, P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.* Vol. **55**, pp. 107–118, 2017.

[66] A. Kumar, J. Singh, D. Singh, R. Dewang, "A historical feedback based misbehavior detection (HFMD) algorithm in VANET," in Proc. *2nd International Conference on Computational Intelligence and Networks (CINE),* IEEE, 2016, pp. 15–22.

[67] A. Wasef, R. Lu, X. Lin, X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks," *IEEE Wireless Commun.* Vol. **17**(5), 2010.

[68] B. Premasudha, V. Ram, J. Miller, R. Suma, "A review of security threats, solutions and trust management in VANETs," *Int. J. Next-Generation Comput.* Vol. 7(1), pp. 38–57, 2016.

[69] B. K Chaurasia, S. Verma, GS. Tomar, "Trust computation in vanets," *International Conference on Communication Systems and Network Technologies (CSNT),* IEEE, 2013, pp. 468–471

[70] T. Krishna, R. Barnwal, S. Ghosh, "MDS-based trust estimation of event reporting node in vanet," *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* IEEE, 2013, pp. 315–320.

[71] W. Li, H. Song, "Art: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transport. Syst.* Vol 17(4), 960–969, 2016.

[72] R. Schmidt, T. Leinmuller, E. Schoch, A. Held, G. Schafer, "Vehicle behavior analysis to enhance security in vanets," in Proc. *4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM08).* IEEE, 2008, pp. 123-135.

[73] A.Wu, J. Ma, S. Zhang, "Rate: a RSU-aided scheme for data-centric trust establishment in vanets," in Proc. *7th International Conference Wireless Communications, Networking and Mobile Computing (WiCOM),* , IEEE, 2011, pp. 1–6.

[74] J. Zhang, "A survey on trust management for VANETs," in Proc. *IEEE International Conference on Advanced Information Networking and Applications (AINA),* IEEE, 2011, pp. 105–112.

[75] S. Ahmed, K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," in proc. *Wireless Communications and Networking Conference (WCNC),* (IEEE, 2016), pp. 1–6.

[76] H. Zhu, X. Lin, R. Lu, P.H Ho, X. Shen,. "Aema: an aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in Proc. *IEEE International Conference* on *Communications (ICC'08)*, 2008, pp. 1436–1440.

[77] L. Yeh, Y.C Lin, "A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks," *IEEE Trans. Intell. Transport. Syst.* Vol. 15(4), 1607–1621, 2014.

[78] R. Lu, X. Lin, X. Liang, X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transport. Syst.* Vol. 13(1), pp. 127–139 , 2012.

[79] A. Boualouache, S.M Senouci, S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surv.* Tutor, 2017.

[80] W. Xu, H. Zhou, N. Cheng, F. Lyu,W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA J. Automatica Sinica*, Vol. 5, no. 1, pp. 19-35, 2018.

[81] X. Zhang, C. Lyu, Z.Shi, D. Li, N. Xiong, C.Chi, "Reliable Mutiservice delivery in Fog Enabled Vanets: Integrated misbehavior section and tolerance," *IEEE Access*, Vol. 7, pp. 95762-95778, 2019.

[82] D. Liu, "Big Data Analytics Architecture for Internet-of-Vehicles Based on the Spark," in Proc. *2018 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, 2018, pp. 13-16.

[83] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, 2017, pp. 591-602.

[84] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960-969, 2016.

[85] T. Cheng, G. Liu, Q. Yang, and J. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 652-663, Mar. 2019.

[86] A. Ullah, X. Yao, S. Shaheen, and H. Ning, "Advances in position based routing towards ITS enabled FoG-oriented VANET-A survey," *IEEE Trans. Intell. Transp. Syst.*, to be published. doi: 10.1109/TITS.2019. 2893067.

[87] S. Sultan, Q. Javaid, E. Rehman, A. Alahmadi, and N. Ullah, "Incentive-Driven Approach for Misbehavior Avoidance in Vehicular Networks," *CMC-Computers, Materials & Continua*, Vol. 70(3), pp. 6089–6106, 2021.

[88] K . Zhang, Y. Mao, S. Leng, A. Vinel, and Y. Zhang, "Delay constrained offloading for mobile edge computing in cloud enabled vehicular networks," in *Proc. 8th Int. Workshop Resilient Netw. Design Modeling*, 2016, pp. 288-294.

[89] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619-15629, 2017.

[90] N. Noorani, S. A. H. Seno, ``Routing in VANETs based on intersection using SDN and fog computing," in *Proc. 8th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, 2018, pp. 339-344.

[91] S. Dahmane, C. A. Kerrache, N. Lagraa, and P. Lorenz, "WeiSTARS: A weighted trust-aware relay selection scheme for VANET," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1-6.

[92] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786-1797, 2017.

[93] L. Cheng, J. Niu, J. Cao, S. K. Das, and Y. Gu, "QoS aware geographic opportunistic routing in wireless sensor networks," *IEEE Trans. ParallelmDistrib. Syst.*, Vol. 25, no. 7, pp. 1864-1875, 2014.

[94] J. Wu, K. Ota, M. Dong, and C. Li, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, pp. 416-424, 2016.

[95] J. Liang, J. Y. Zhu, and R. Yu, "A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position," *Applied Soft Computing.*, vol. 75, pp. 712-727, 2019.

[96] X. Wen, L. Shao, Y. Xue, and W. Fang, "A rapid learning algorithm for vehicle classi_cation," *Inf. Sci.*, Vol. 295, pp. 395-406, 2015.

[97] H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "A security aware fuzzy enhanced reliable ant colony optimization routing in vehicular ad hoc networks," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, 2018, pp. 1071-1078.

[98] A. M. Vegni and T. D. C. Little, "A message propagation model for hybrid vehicular communication protocols," in *Proc. 7th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Newcastle Upon Tyne, U.K., 2010, pp. 382-386.

[99] S. M. Zin, N. B. Anuar, M. L. M. Kiah, and I. Ahmedy, "Survey of secure multipath routing protocols for WSNs," *J. Netw. Comput. Appl.*, Vol. 55, pp. 123-153, 2015.

[100] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," *J. Netw. Comput. Appl.*, vol. 33, no. 4, pp. 422-432, 2010.

[101] D. Han and J. M. Chung, "Self-similar traf_c end-to-end delay minimization multipath routing algorithm," *IEEE Commun. Lett.*, vol. 18, no. 12, pp. 2121-2124, 2014.

[102] Y. Challal, A. Ouadjaout, N. Lasla, M. Bagaa, and A. Hadjidj, "Secure and ef_cient disjoint multipath construction for fault tolerant routing in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 34, pp. 1380-1397, 2011.

[103] A. S. Lal and R. Nair, "Region authority based collaborative scheme to detect Sybil attacks in VANET" in *Proc. Int. Conf. Control Commun. Comput. India (ICCC)*, 2015, pp. 664-668.

[104] P . P. C. Lee, V. Misra, and D. Rubenstein, "Distributed algorithms for secure multipath routing in attack-resistant networks," *IEEE/ACM Trans. Netw.*, vol. 15, no. 6, pp. 1490-1501, 2007.

[105] Y . Cao, F. Song, Q. Liu, M. Huang, H. Wang, and I. You, "A LDDoS- Aware energy-efficient multipathing scheme for mobile cloud computing systems," *IEEE ACCESS*, vol. 5, pp. 21862-21872, 2017.

[106] P. M. Mohan, T. J. Lim, and M. Gurusamy, " Fragmentation-based multi-path routing for attack resilience in software defined networks," in *Proc.IEEE 41st Conf. Local Comput. Netw. (LCN)*, Dubai, UAE, 2016, pp. 583-586.

[107] M . Saad, A. Leon-Garcia, and W. Yu, "Optimal network rate allocation under end-to-end quality-of-service requirements," *IEEE Trans. Netw. Service Manage.*, vol. 4, no. 3, pp. 40_49, 2007.

[108] W. H. Wang, M. Palaniswami, and S. H. Low, "Application-oriented flow control: Fundamentals, algorithms and fairness," *IEEE/ACM Trans. Netw.*, vol. 14, no. 6, pp. 1282_1291, 2006.

[109] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, Vol. 10, no. 10, pp. 3528-3540, 2011.

[110] J. Jin, M. Palaniswami, and B. Krishnamachari, "Rate control for heterogeneous wireless sensor networks: Characterization, algorithms and performance," *Comput. Netw.*, vol. 56, pp. 3783-3794, 2012.

[111] N.J. Habeeb, S.T. Weli, Relationship of smart cities and smart tourism: an overview. *HighTech Innovat J*, Vol. 1 (4), pp. 194-202, 2020.

[112] M. Sichitiu, M. Kihl, "Inter-vehicle communication systems: A survey." *IEEE Communications Surveys & Tutorials*, Vol. 10(2), pp. 88-105, 2008.

[113] S. Tanzila, S. Tariq, R. Amjad, M. Zahid, and J. Qaisar, "Intrusion Detection System Through Advance Machine Learning for the Internet of Things Networks." *IT Professional*, Vol. 23(2), pp. 58-64, 2021.

[114] K. Gu, X. Dong, W. Jia, Malicious node detection scheme based on correlation of data and network toplogy in fog-computing based VANETs." *IEEE Transaction on Cloud Computing*, Vol. 5(2), pp. 1-18, 2020.

[115] R. Hussain, F. Hussain, S. Zeadally, "Integration of VANET and 5G security: A review of design and implementation issues." *Future generation computer systems*, Vol. 101(3), pp. 843-864, 2019.

[116] D. Manivannan, M. Shawkat, S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)." *Vehicular Communications*, Vol. 25(2), pp. 1-18, 2020.

[117] S. A. Siddique, A. Mahmood, Q.Z. Sheng, H. Suzuki, W. Ni, "A survey of trust management in the internet of vehicles," *Electronics*, Vol. 10, 2223, 2021.

[118] C. Huang, R. Lu, K.K.R. Choo, "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges." *IEEE Communications Magazine*, Vol. 55(11), pp. 105-111, 2017.

[119] M. Mukherjee, M. Matam, Shu, "Security and privacy in fog computing: Challenges." *IEEE Access, Vol.* 5, pp. 19293-19304, 2017.

[120] F. Bonomi, "Connected vehicles, the internet of things, and fog computing." *The eighth ACM international workshop on vehicular internetworking (VANET),* pp.13-15, 2011.

[121] A. Iftikhar, H.K Zawar, G. Aaron, S. Khurram, M.A.K. Khattak, M.A.K., A. Murtaza, M. Nasru. "Macroscopic Traffic Flow Characterization at Bottlenecks." *Civil Engineering Journal,* Vol. 6(7), pp. 1227–1242, 2020.

[122] G. Rehman, A. Ghani, M. Zubair, I. Saeed, D. Singh, "SOS: Socially omitting selfishness in IoT for smart and connected communities." *International Journal of communication systems,* Vol. 1(25), pp. 1-16, 2020.

[123] M. Hasan S. Mohan, T. Shimizu, H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms." *IEEE transactions on intelligent vehicles*, Vol. 25(1), pp. 1-22, 2020.

[124] M.V. De, R. Brundo, I. Brandic, Energy and profit aware proof-of-stake offloading in blockchain-based VANETs. *Proceedings of 12th IEEE/ACM international conference on utility and cloud computing UCC 19,* pp. 177-186, 2019.

[125] N.C. Velayudhan, A. Anitha, M. Madanan, V. Paul, "Review on avoiding Sybil in VANET while operating in an urban environment." *Journal of Theoretical and Applied Information Technology*, Vol. 97(20), 2019..

[126] A. Zouinkhi, A. Ltifi, C. Chouaib, M. Naceur, " A trust management based on cooperative scheme in VANET," *International Journal of Information and Communication Technology*, Vol.13 No.3, pp.291 - 304, 2012.

[127] R.W. Van-der-Heijden, F. Kargl, O.M. Abu-Sharkh, A. Al-Momani, "Enhanced position verification for vanets using subjective logic." *IEEE 84th Vehicular Technology Conference (VTC-Fall),* pp. 1-7, 2016.

[128] A. Rrecaj, V. Alimehaj, M. Malenkovska, C. Mitrovski, "An Improved CTM model for urban signalized intersections and exploration of traffic evaluation." *Civil Engineering Journal*, Vol. 7(2), pp. 357-375, 2021.

[129] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A robust and privacy-preserving reputation management scheme for pseudonym enabled VANETs," *Int. J. Distrib. Sensor Netw.*, vol. 1(16), Art. no. 6138251, 2016.

[130] U . F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular

networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407-420, 2011.

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

[132] D. B. Rawat, B. 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, 2011, pp. 146-151.

[133] O . A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on Dempster-Shafer for detecting misbehaving vehicles," *Comput. Commun.*, vol. 41, pp. 43-54, 2014.

[134] A. El Khatib, A. Mourad, H. Otrok, O. A. Wahab, and J. Bentahar, "A cooperative detection model based on artificial neural network for VANET QoS-OLSR protocol," in proc. *IEEE ICUWB*, Montreal, QC, Canada, 2015, pp. 1-5.

[135] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM based intelligent detection model for clustered vehicular ad hoc networks," *Expert Syst. Appl.*, vol. 50, pp. 40-54, 2016.

[136] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen, C. Sun, "DAPV: Diagnosing Anomalies in MANETs Routing With Provenance and Verification," *IEEE Access*, Vol. 7, pp. 35302–35316, 2019.

[137] J. Wilson,K. Subramaniam, "Improved multi objective data transmission using conventional route selection algorithm in mobile ad hoc network," *Peer-to-Peer Networking and Applications*, Vol. 13, pp. 1091–1101 2020.

[138] S. Du, J. Hou, S. Song, Y. Song, Y. Zhu, "A geographical hierarchy greedy routing strategy for vehicular big data communications over millimeter wave," *Physical Communication*, Vol. 40, pp. 1–9, 2020.

[139] W. Fang, W. Zhang, W. Chen, Y. Liu, C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Networks*, Vol. 26, pp. 3169–3182 2020.

[140] T.K. Saini, S.C. Sharma, "Recent advancements, review analysis, and extensions of the aodv with the illustration of the applied concept," *Ad Hoc Networks*, Vol. 103, pp. 1–20, 2020.

[141] H. Kojima, N. Yanai, J.P. Cruz, "ISDSRC: Improving the security and availability of secure routing protocol," *IEEE Access* Vol. 7, pp. 74849–74868, 2019.

[142] Y. Park, C. Sur, K.H. Rhee, "A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency," *Security and Communication Network*, Vol. 18, pp. 1-13, 2018.

[143] A. Sharma, E.S. Pilli, A.P. Mazumdar, P. Gera, "Towards trustworthy internet of things: A survey on trust management applications and schemes," *Computer Communications*, Vol. 160, pp. 475–493, 2020.

[144] R.K. Chahal, N. Kumar, S. Batra, "Trust management in social internet of things: A taxonomy, open issues, and challenges," *Computer Communications*, Vol. 150, pp. 13–46. 2020.

[145] R.J. Cai, X.J. Li, P.H.J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," *IEEE Transactions on Mobile Computing*, Vol. 18(1), pp. 42–55, 2019.

[146] S.N. Mahapatra, B.K. Singh, V. Kumar, "A survey on secure transmission in internet of things: Taxonomy, recent techniques, research requirements, and challenges," *Arabian Journal for Science and Engineering*, Vol. 45, pp. 6211–6240, 2020.

[147] M.A. Qurashi, C.M. Angelopoulos, V. Katos, "An architecture for resilient intrusion detection in ad-hoc networks," *Journal of Information Security and Applications*, Vol. 53, pp. 1–12, 2020.

[148] H. Riasudheen, H., K. Selvamani, S. Mukherjee, M. Divyasree, "An efficient energy-aware routing scheme for cloud-assisted manets in 5G," *Ad Hoc Networks*, Vol. 97, pp. 1–22, 2020.

[149] H. Xu, et al "Trust-based probabilistic broadcast scheme for mobile ad hoc networks," *IEEE Access*, Vol. 8, pp. 21380–21392, 2020.

[150] P. Theerthagiri, "FUCEM: futuristic cooperation evaluation model using markov process for evaluating node reliability and link stability in mobile ad hoc network," *Wireless Networks*, Vol. 26, pp. 4173–4188, 2020.

[151] N. Djedjig, D. Tandjaoui, F. Medjek, I. Romdhani, "Trust-aware and cooperative routing protocol for iot security," *Journal of Information Security and Applications*, Vol. 52, pp. 1–17, 2020.

[152] R.H. Jhaveri, N.M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," *International Journal of Communication Systems*, Vol. 30, pp. 1–24, 2016.

[153] A.M. Desai, R.H. Jhaveri, "Secure routing in mobile Ad hoc networks: a predictive approach," *International Journal of Information Technology volume*, Vol. 11, pp. 345–356, 2018.

[154] R.H. Jhaveri, A. Desai, A. Patel, Y. Zhong, "A Sequence Number Prediction Based Bait Detection Scheme to Mitigate Sequence Number Attacks in MANETs," *Security and Communication Networks, Wiley-Hindawi*, 1–13, 2018.

[155] L. Chen, Q. Li, K. M. Martin, "Private reputation retrieval in public-a privacy-aware announcement scheme for VANETs," *IET Inf. Secur.* Vol. 11(4), pp. 204–210, 2016.

[156] Z. Lu, Q. Wang, G. Qu, Z. Liu, "BARS: a blockchain-based anonymous reputation system for trust management in VANETs" in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)., IEEE, New York*, pp. 98–103, 2018.

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

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

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

[160] 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.

[161] 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.

[162] R. Sun, Y. Huang, L. Zhu, "Communication by Credence Credit based: Trust Communication in Vehicular Ad Hoc Networks," *Mobile Netw Appl.*, Vol. 71, pp. 1-13, 2021.

[163] P. Sankar, A. Kumar, B. Bharathi. "Blockchain-Based Incentive Announcement In Vanet Using CreditCoin". *Advances in Electronics, Communication and Computing.*, Vol. 709. pp. 567-574, 2021.

[164] 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.

[165] L. Alouache, N. Nguyen, M. Aliouat, R. Chelouah, "Credit Based Incentive Approach for V2V Cooperation in Vehicular Cloud Computing," *Internet of Vehicles*, Vol. 11253, 2018.

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

[167] G. Zhao, M. Chen, X. Wei, "RIS: A reciprocal incentive scheme in selfish opportunistic networks," *Wirel. Pers. Commun.*, Vol. 70, pp. 1711–1734, 2013.

[168] H. Liu, P.C Lee, J.C.S. Lui, "On the credit evolution of credit-based incentive protocols in wireless mesh networks," *Comput. Netw.*, Vol. 57, pp. 3327–3343, 2013.

[169] T. Seregina, O. Brun, R. El-Azouzi, B.J. Prabhu, "On the design of a reward-based incentive mechanism for delay tolerant networks," *IEEE Trans. Mob. Comput.* Vol. 16, pp. 453–465, 2017.

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

[171] J. Li, X.Wang, R. Yu, "Reputation-based incentives for data dissemination in mobile participatory sensing networks,"*Int. J. Distrib. Sens. Netw.* Vol.11, pp. 172130, 2015.

[172] A. Katmada, A. Satsiou, I. Kompatsiaris, "A reputation-based incentive mechanism for a crowdsourcing platform for financial awareness,"In Proc. *International Workshop on the Internet for Financial Collective Awareness and Intelligence (IFIN 2016),* Florence, Italy, pp. 57–80, 2016.

[173] Y. Zhan, Y. Xia, J. Zhang, Y. Wang, "Incentive mechanism design in mobile opportunistic data collection with time sensitivity," *IEEE Int. Things J.*, Vol. 5, pp. 246–256, 2018.

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

[175] M. Louta, P. Bellavista, "Bringing always best connectivity vision a step closer: challenges and perspectives," *IEEE Commun. Mag.*, Vol. 51 (2), pp. 158–166, 2013.

[176] P. Resnick, K. Kuwabara, R. Zeckhauser, *et al.* "Reputation systems," *Commun. ACM*, Vol. 43(12), pp. 45–48, 2000.

[177] G. Dini, A.L Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network," *Ad Hoc Netw.*, Vol. 10(7), pp. 1167–1178, 2012.

[178] R. Chen, F. Bao, M. Chang, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distrib. Syst.*, Vol. 25(5), pp. 1200–1210, 2014.

[179] Y. Zhu, B. Xu, X. Shi, X, "A survey of social-based routing in delay tolerant networks: positive and negative social effects," *IEEE Commun. Surv. Tutor.*, Vol. 15(1), pp. 387–401, 2013.

[180] N. Chakchouk, "A survey on opportunistic routing in wireless communication networks," *IEEE Commun. Surv. Tutor.*, Vol. 17(4), pp. 2214–2241, 2015.

[181] S. Kraounakis, I.N. Demetropoulos, A. Michalas,"A robust reputation-based computational model for trust establishment in pervasive systems," *IEEE Syst. J.*, Vol. 9(3), pp. 878–891, 2015.

[182] X. Li, F. Zhou, X. Yang, "Scalable feedback aggregating (sfa) overlay for large-scale p2p trust management," *IEEE Trans. Parallel Distrib. Syst.*, Vol. 23(10), pp. 1944–1957, 2012.

[183] M. Eirinaki, M.D. Louta, I. Varlamis, "A trust-aware system for personalized user recommendations in social networks," *IEEE Trans. Syst. Man Cybern., Syst.*, Vol. 44(4), pp. 409–421, 2014.

[184] I. Varlamis, M. Eirinaki, M. Louta, "Application of social network metrics to a trust-aware collaborative model for generating personalized user recommendations," *Influence Technol. Social Netw. Anal. Mining*, Vol. 6, pp. 49–74, 2013.

[185] G. Zhan, W. Shi, J. Deng, "Design and implementation of tarf: a trust-aware routing framework for wsns', *IEEE Trans. Dependable Secur. Comput.*, Vol. 9(2), pp. 184–197, 2012.

[186] S. Bera, S. Misra, S.K. Roy, "Softwsn: software-defined wsn management system for iot applications," *IEEE Syst. J.*, Vol. PP(99), pp. 1–8, 2016.

[187] S. Sicari, A. Rizzardi, L.A. Grieco, "Security, privacy and trust in internet of things: the road ahea," *Comput. Netw.*, Vol. 76, pp. 146–164, 2015.

[188] S. Ruohomaa, L. Kutvonen, "Trust management survey," '*ITrust*' Vol. 3477, pp. 77–92, 2005.

[189] S. Trifunovic, F. Legendre, "Trust in opportunistic networks," *Comput. Eng. Netw. Lab.*, pp. 1–12, 2009.

[190] K. Wei, X. Liang, K. Xu, "A survey of social-aware routing protocols in delay tolerant networks: applications, taxonomy and design-related issues," *IEEE Commun. Surv. Tutor.*, Vol. 16, (1), pp. 556–578, 2014.

[191] W. Moreira, P. Mendes, "Social-aware opportunistic routing: the new trend," *Routing in Opportunistic Networks*' Springer, pp. 27–68, 2013.

[192] K. Hoffman, D. Zage, C. Nita-Rotaru,"A survey of attack and defense techniques for reputation systems," *ACM Comput. Surv. (CSUR)*, Vol. 42 (1), p. 1-13, 2009.

[193] R. Kerr, R. Cohen, "Smart cheaters do prosper: defeating trust and reputation systems," In Proc. of the *8th Int. Conf. Autonomous Agents and Multiagent Systems-Volume 2. Int. Foundation for Autonomous Agents and Multiagent Systems*, 2009, pp. 993–1000.

[194] A. Josang, J. Golbeck, "Challenges for robust trust and reputation systems," in Proc. of the *5th Intl. Workshop on Security and Trust Management (SMT 2009)*, Saint Malo, France, 2009, pp. 52-62.

[195] Q. Jiang, C. Men, H. Yu, "A secure credit-based incentive scheme for opportunistic networks," in Proc. *7th Int. Conf. Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, 2015, vol. 1, pp. 87–91.

[196] A. Sharma, "A credit based routing mechanism to contrast selfish nodes in delay tolerant networks," in Proc. *Int. Conf. Parallel, Distributed and Grid Computing (PDGC)*, 2014, pp. 295–300.

[197] A. Jesudoss, S.V. Kasmir, A. Sulaiman "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme" *Ad Hoc Networks*, Vol. 24, pp. 250–263, 2015.

[198] R.P.Nayak, S. Sethi, S.K. Bhoi, et al. "ML-MDS: Machine Learning based Misbehavior Detection System for Cognitive Software-defined Multimedia VANETs (CSDMV) in smart cities" *Multimed Tools Appl.* pp. 35-41, 2022.

[199] M. M. Hamdi, M. Dhafer, A. S. Mustafa, S. A. Rashid, A. J. Ahmed and A. M. Shantaf, "Effect Sybil attack on security Authentication Service in VANET," in Proc. *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-6, 2022.

Bibliography

[1] Dedicated Short Range Communication working group, "*Dedicated Short Range Communications*".http://grouper.ieee.org/groups/scc32/dsrc/index.html, outline, 2015.

[2] S. Grafling, P. Mahonen, J. Riihijarvi, "Performance evaluation of IEEE 1609 WAVE and IEEE 802.11p for vehicular communications," in Proc. *Second Inter-national Conference on Ubiquitous and Future Networks (ICUFN),* 2010, IEEE, pp. 344–348.

[3] S. Eichler, "Performance evaluation of the IEEE 802.11 p WAVE communication standard, in *Proc 66th Vehicular Technology Conference, 2007. VTC-2007,* IEEE, pp.2199–2203.

[4] A . Dua, N. Kumar, S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Veh. Commun.*, Vol. 1(1), pp. 33–52, 2014.

[5] F. Li, Y. Wang, "Routing in vehicular ad hoc networks: a survey," *IEEE Veh. Technol. Mag.*, Vol.2 No.2, pp. 12-22, 2007.

[6] A. Gainaru, C. Dobre, V. Cristea, "A realistic mobility model based on social networks for the simulation of VANETs," in *Proc. IEEE 69th Vehicular Technology Conference, 2009, VTC* IEEE, 2009, pp.1–5.

[7] J. Sun, Y. Fang, "Defense against misbehavior in anonymous vehicular ad hoc networks," *Ad Hoc Netw.*, Vol. 7(8), pp. 1515–1525, 2009.

[8] J.M. Pozo, O. Trullols, J.M. Barceló, J.G. Vidal, "A cooperative ARQ for delay-tolerant vehicular networks," in *Proc. 28th International Conference on Distributed Computing Systems Workshops, ICDCS'08,* IEEE, 2008, pp.192–197.

[9] L. Aparecido, "Data dissemination in vehicular networks: challenges, solutions, and future perspectives," in *Proc. 7th International Conference on New Technologies, Mobility and Security (NTMS),* IEEE, 2015, pp.1–5.

[10] S. Yousefi, M.S. Mousavi, M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," in *Proc. 6th International Conference on ITS Telecom-munications Proceedings, IEEE,2006,* pp.761–766.

[11] B. Paul, M. Ibrahim, M. Bikas, A. Naser, "Vanet routing protocols: pros and cons," *International journal of computer applications*, Vol. 20, No. 3, pp.1-12, 2011.

[12] J. Park, Y.S. Jeong, S. Park, H.C. Chen, "Embedded and Multimedia Computing Technology and Service," *Lecture Notes in Electrical Engineering,* Springer, Vol.181, 2012.

[13] R. van der Heijden, S. Dietzel, F. Kargl, "Misbehavior detection in vehicular ad-hoc networks," in *Proc. 1st GI/ITG Inter-Vehicle Communication, Institute of Distributed Systems*, 2013, pp. 102-114.

[14] A. Daeinabi, A. Ghaffarpour, "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks," *Multimed Tools Appl.* Vol. 1(78), pp. 325–338, 2013.

[15] P. Sangulagi, M. Sarsamba, V. Katgi, "Recognition and Elimination of Malicious Nodes in Vehicular Ad Hoc Networks (VANET's)," *Indian Journal of Computer Science and Engineering (IJCSE).* Vol.2 (4), pp 16-22, 2013.

[16] N. Haddadou, A. Rachidi. Y.Ghamri-Doudane, "Trust And Exclusion In Vehicular Ad Hoc Network : An Economic Incentive Model Based Approach," *IEEE Transaction.* IEEE, pp 13-18, 2013.

[17] N. Haddadou, A. Rachidi. Y.Ghamri, "A Job Market Signaling Approach Scheme for Incentive and Trust Management in Vehicular Ad Hoc Network," *IEEE Transactions on Vehicular Technology*, Vol. 64, NO. 8, IEEE, pp 3657-3674, 2015.

[18] Z. Huang, A. Marcos Cavenaghi, M. Stojmenovic, "A social network approach to trust management in VANETs," *Peer-to-Peer Netw. Appl.*, Springer, Vol.7, pp 229-242, 2014.

[19] U Khan, S Agrawal, S Silakari, "A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks," *Information Systems Design and Intelligent Applications.*, Springer, Vol. 15(2), pp. 45-56, 2015.

[20] R. W van der Heijden, S. Dietzel, T. Leinmuller, F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems,".1610.06810 Springer, *2016.*

[21] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari and A. Tyagi, "Vehicular Security through Reputation and Plausibility Checks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 384-394, 2014.

[22] S. Ruj, M.A Cavenaghi, Z. Huang, A. Nayak, "Data-Centric Misbehavior Detection in VANETs," in Proc. *Vehicular Technology Conference (VTC Fall), 2011, IEEE.* IEEE, pp. 1–5.

[23] Y. Hua Ho, C. Han Lin, L. Jyh Chen, "On-demand Misbehavior Detection for Vehicular Ad Hoc Network," *International Journal of Distributed Sensor Networks* (IJDSN)., Vol. 12(10). pp. 1-14 , 2016.

[24] W. Liang, Z. Li, H. Zhang, S. Wang, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges and Trends," *International Journal of Distributed Sensor Networks IJDSN.*, Vol 11. No. 8, pp. 745303, 2015.

[25] M. Arshad, Z. Ullah, H. Criuck shank, Y. Cao, "A survey of local/cooperative based malicious information detection techniques in VANETs," *Journal on Wireless Communications and Networking,* Vol. 62(18), pp-1-24, 2018.

[26] J.Molina-Gil, P. Caballero-Gil, C. Caballero-Gil, "Countermeasures to prevent misbehaviour in VANETs," *J. UCS.,* Vol. 18(6), pp. 857–873, 2012.

[27] E. Hernandez-Orallo, D. Olmos, C. Cano, T. Calafate, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," *IEEE Transactions on Mobile Computing.,* Vol. 14, No. 6. IEEE. pp. 1162-1175, 2015.

[28] L. ChauHua, M. Hossein, Y. PorLip, "Social networking-based cooperation mechanisms in vehicular ad-hoc network-a survey," *Vehicular Communications.,* Vol. 10 (17), pp 57-73, 2017.

[29] T.J Kim, A. Studer, R. Dubey, X. Zhang, A. Perrig, F. Bai, B. Bellur, A. Iyer, "VANET alert endorsement using multisource filters ACM," in Proc. *Seventh ACM International Workshop on VehiculArInterNETworking.*, 2010, pp. 51–60.

[30] T . Zaidi, S. Giri, S. Chaurasia, "Malicious Node Detection through AODV in VANET," *International Journal of Ad hoc, Sensor &Ubiquitous Computing.*, Vol.9, No. 2, pp. 33-43, 2018.

[31] A. Vulimiri, A. Gupta, P. Roy, S. Muthaiah, A. Kherani,. "Application of secondary information for misbehavior detection in VANETs," In Proc. *International Conference on Research in Networking.*, 2010, pp. 385–396.

[32] K. Sha, S. Wang, W. Shi, "*RD*4: Role-differentiated cooperative deceptive data detection and filtering in vanets," *IEEE Trans. Veh. Technol.* Vol. 59(3), pp. 1183–1190, 2010.

[33] J. Rezgui, S. Cherkaoui, "Detecting faulty and malicious vehicles using rule-based communications data mining," in Proc. *36thIEEE Conference Local Computer Networks (LCN),*2011, pp. 827–834.

[34] D. Huang, S. Williams, S. Shere, "Cheater detection in vehicular networks," in Proc. *IEEE 11th Trust, Security and Privacy in Computing and Communications (TrustCom), International Conference.,* 2012, pp. 193–200.

[35] K. Zaidi, M. Milojevic, V. Rakocevic, M. Rajarajan, "Data-centric rogue node detection in vanets," in Proc. *13th International Conference on Trust, Security and Privacy in Computing and Communications.* IEEE, 2014, pp. 398–405.

[36] K. Zaidi, M. Milojevic, V. Rakocevic, A. Nallanathan, M. Rajarajan, "Host-based intrusion detection for vanets: a statistical approach to rogue node detection," *IEEE Trans. Veh. Technol.*,Vol. 65(8), pp. 6703–6714, 2019.

[37] R.W Van der Heijden, F. Kargl, OM. Abu-Sharkh, A. Al-Momani, "Enhanced position verification for vanets using subjective logic," In Proc. *IEEE Vehicular Technology Conference*, 2016, Universitat Ulm.

[38] SK. Harit, G. Singh, N. Tyagi, " Fox-hole model fordata-centric misbehaviour detection in vanets," In Proc. *Third International Conference* on *Computer and Communication Technology(ICCCT)*, IEEE, 2012, pp. 271–277.

[39] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs. in Proc. *1st ACM International Workshop on Vehicular Ad Hoc Networks*. ACM, 2004, pp. 29–37.

[40] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, JP. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Selected Areas Commun*. Vol. 25(8) , 2007.

[41] A. Rivero Garcia, I. Santos Gonzalez, P. Caballero Gil, C. Caballero Gil, "Vanet event verification based on user trust," in Proc. *24th Euro micro International Conference On Parallel, Distributed, and Network-Based Processing (PDP)*, IEEE, 2016, pp. 313–316.

[42] B. Płaczek, M. Bernas, "Detection of malicious data in vehicular ad hoc networks for traffic signal control applications," in Proc. *International Conference on Computer Networks*.. Springer, 2017, pp. 72–82.

[43] H. Al Falasi, N. Mohamed, H. El-Syed, "Similarity based trust management system: data validation scheme," *Hybrid Intelligent Systems*. Springer, pp. 141–153,2016.

[44] N. Fan, Q. Wu, "Trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Networks,* Elsevier, 2018, pp 1-13.

[45] H . Hasrouny, A. Ellatif Samhat, C. Bassilc, A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications.*, Elsevier, Vol. 7(2017), pp. 7-20, 2017.

[46] Z. Soltani, K. Mizanian "Misbehavior Node Detection in Vehicular ad-hoc Networks: A survey, With Special Emphasis on Multihop Broadcast Protocols," *Researcher* Vol. 9(1), pp. 41-46, 2017.

[47] C.H Kim, I.H Bae, "A misbehavior-based reputation management system for VANETs," *Embedded and Multimedia Computing Technology and Service.*, Springer, pp. 441–450, 2012.

[48] A. Ahmed, kamalrunizam, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," *Frontiers of Computer Science.*, Springer, Vol. 9(2), pp.280–296, 2015.

[49] Santos J., L.M., Moreira, E. "|An evaluation of reputation with regard to the opportunistic forwarding of messages in VANETs,"| *J Wireless Com Network*, Vol. 204, 2019.

[50] K. Govindan, P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Commun. Surv. Tutorials.* Vol. 14(2), pp. 279–298 , 2012.

[51] R. van der Heijden, S. Dietzel, F. Kargl, "Misbehavior detection in vehicular ad-hoc networks," in Proc. *1st Fachgesprach Inter-Vehicle Communication (FG-IVC 2013*, pp. 201-223.

[52] T. Lu, S. Chang, and W. Li, "Fog computing enabling geographic routing for urban area vehicular network," *Peer Peer Netw. Appl.*, vol. 11, no. 4, pp. 749-755, 2018.

[53] A. Ltifi, A. Zouinkhi, M. Bouhlel, "An Alert Endorsement through Cooperative Trust Management for VANET," *International Journal of Computer Science and Information Security (IJCSIS).* Vol. 10. No.4, 2012.

[54] N. Bismeyer, S. Mauthofer, KM. Bayarou, F. Kargl, "Assessment of node trustworthiness in vanets using data plausibility checks with particle filters," In Proc. *Vehicular Networking Conference (VNC),* IEEE, 2012, pp. 78–85.

[55] R. Abassi, C. Ben, and D. Sauveron, "TSME: a trust-based security scheme for message exchange in vehicular Ad hoc networks," *Hum. Cent. Comput. Inf. Sci.* Vol. 10, No. 43, 2020.

[56] Z. Cao, J. Kong, U. Lee, M. Gerla, Z. Chen, "Proof-of-relevance: filtering false data via authentic consensus in vehicle ad-hoc networks," In Proc. *INFOCOM Workshops* IEEE, 2008, pp. 1–6.

[57] F. Dotzer, L. Fischer, P. Magiera, "A. Vars: A vehicle ad-hoc network reputation system," in Proc. *Sixth IEEE International Symposium World of Wireless Mobile and Multimedia Networks., WoWMoM* .IEEE, 2005, pp. 454–456.

[58] N. W Lo, H.C Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP J. Wirel. Commun. Netw.*, Vol. 1, pp. 25-48, 2009.

[59] Q. Ding, X. Li, M. Jiang, X. Zhou, "Reputation-based trust model in vehicular ad hoc networks," in Proc. *International Conference on Wireless Communications and Signal Processing (WCSP),* IEEE, 2010, pp. 1–6.

[60] Z. Huang, S. Ruj, M. Cavenaghi, A. Nayak, "Limitations of trust management schemes in VANET and countermeasures," In Proc. *22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC),* IEEE, 2011, pp. 1228–1232

[61] D. Aniket, "Review of Effective Trust Management Systems in VANET Environments," *International Journal of Grid and Distributed Computing*, Vol. 14. Pp. 1771-1780. 2021.

[62] Z. Abdulkader, A. Abdullah, M. Abdullah, Z. Zukarnain, "Vehicular ad hoc networks and security issues: survey," *Modern Appl. Sci.* Vol. 11(5), No. 30, 2017.

[63] D. Zhang, F. Yu, Z. Wei, A. Boukerche, "Software-defined vehicular ad hoc networks with trust management," In Proc. *6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*. ACM, 2016, pp. 41–49.

[64] A. Alkalbani, A. Tap, T. Mantoro, "Energy consumption evaluation in trust and reputation models for wireless sensor networks," in Proc. *5th International Conference on Information and Communication Technology for the Muslim World (ICT4M),* IEEE, 2013, pp. 1–6.

[65] X. Yao, X. Zhang, H. Ning, P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.* Vol. **55**, pp. 107–118, 2017.

[66] A. Kumar, J. Singh, D. Singh, R. Dewang, "A historical feedback based misbehavior detection (HFMD) algorithm in VANET," in Proc. *2nd International Conference on Computational Intelligence and Networks (CINE),* IEEE, 2016, pp. 15–22.

[67] A. Wasef, R. Lu, X. Lin, X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks," *IEEE Wireless Commun.* Vol. **17**(5), 2010.

[68] B. Premasudha, V. Ram, J. Miller, R. Suma, "A review of security threats, solutions and trust management in VANETs," *Int. J. Next-Generation Comput.* Vol. 7(1), pp. 38–57, 2016.

[69] B. K Chaurasia, S. Verma, GS. Tomar, "Trust computation in vanets," *International Conference on Communication Systems and Network Technologies (CSNT),* IEEE, 2013, pp. 468–471

[70] T. Krishna, R. Barnwal, S. Ghosh, "MDS-based trust estimation of event reporting node in vanet," *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* IEEE, 2013, pp. 315–320.

[71] W. Li, H. Song, "Art: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transport. Syst.* Vol 17(4), 960–969, 2016.

[72] R. Schmidt, T. Leinmuller, E. Schoch, A. Held, G. Schafer, "Vehicle behavior analysis to enhance security in vanets," in Proc. *4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM08).* IEEE, 2008, pp. 123-135.

[73] A.Wu, J. Ma, S. Zhang, "Rate: a RSU-aided scheme for data-centric trust establishment in vanets," in Proc. *7th International Conference Wireless Communications, Networking and Mobile Computing (WiCOM),* , IEEE, 2011, pp. 1–6.

[74] J. Zhang, "A survey on trust management for VANETs," in Proc. *IEEE International Conference on Advanced Information Networking and Applications (AINA),* IEEE, 2011, pp. 105–112.

[75] S. Ahmed, K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," in proc. *Wireless Communications and Networking Conference (WCNC),* (IEEE, 2016), pp. 1–6.

[76] H. Zhu, X. Lin, R. Lu, P.H Ho, X. Shen,. "Aema: an aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in Proc. *IEEE International Conference* on *Communications (ICC'08)*, 2008, pp. 1436–1440.

[77] L. Yeh, Y.C Lin, "A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks," *IEEE Trans. Intell. Transport. Syst.* Vol. 15(4), 1607–1621, 2014.

[78] R. Lu, X. Lin, X. Liang, X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transport. Syst.* Vol. 13(1), pp. 127–139 , 2012.

[79] A. Boualouache, S.M Senouci, S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surv.* Tutor, 2017.

[80] W. Xu, H. Zhou, N. Cheng, F. Lyu,W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA J. Automatica Sinica*, Vol. 5, no. 1, pp. 19-35, 2018.

[81] X. Zhang, C. Lyu, Z.Shi, D. Li, N. Xiong, C.Chi, "Reliable Mutiservice delivery in Fog Enabled Vanets: Integrated misbehavior section and tolerance," *IEEE Access*, Vol. 7, pp. 95762-95778, 2019.

[82] D. Liu, "Big Data Analytics Architecture for Internet-of-Vehicles Based on the Spark," in Proc. *2018 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, 2018, pp. 13-16.

[83] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, 2017, pp. 591-602.

[84] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960-969, 2016.

[85] T. Cheng, G. Liu, Q. Yang, and J. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 652-663, Mar. 2019.

[86] A. Ullah, X. Yao, S. Shaheen, and H. Ning, "Advances in position based routing towards ITS enabled FoG-oriented VANET-A survey," *IEEE Trans. Intell. Transp. Syst.*, to be published. doi: 10.1109/TITS.2019. 2893067.

[87] S. Sultan, Q. Javaid, E. Rehman, A. Alahmadi, and N. Ullah, "Incentive-Driven Approach for Misbehavior Avoidance in Vehicular Networks," *CMC-Computers, Materials & Continua,* Vol. 70(3), pp. 6089–6106, 2021.

[88] K . Zhang, Y. Mao, S. Leng, A. Vinel, and Y. Zhang, "Delay constrained offloading for mobile edge computing in cloud enabled vehicular networks," in *Proc. 8th Int. Workshop Resilient Netw. Design Modeling*, 2016, pp. 288-294.

[89] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619-15629, 2017.

[90] N. Noorani, S. A. H. Seno, ``Routing in VANETs based on intersection using SDN and fog computing," in *Proc. 8th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, 2018, pp. 339-344.

[91] S. Dahmane, C. A. Kerrache, N. Lagraa, and P. Lorenz, "WeiSTARS: A weighted trust-aware relay selection scheme for VANET," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1-6.

[92] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786-1797, 2017.

[93] L. Cheng, J. Niu, J. Cao, S. K. Das, and Y. Gu, "QoS aware geographic opportunistic routing in wireless sensor networks," *IEEE Trans. ParallelmDistrib. Syst.*, Vol. 25, no. 7, pp. 1864-1875, 2014.

[94] J. Wu, K. Ota, M. Dong, and C. Li, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, pp. 416-424, 2016.

[95] J. Liang, J. Y. Zhu, and R. Yu, "A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position," *Applied Soft Computing.*, vol. 75, pp. 712-727, 2019.

[96] X. Wen, L. Shao, Y. Xue, and W. Fang, "A rapid learning algorithm for vehicle classi_cation," *Inf. Sci.*, Vol. 295, pp. 395-406, 2015.

[97] H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "A security aware fuzzy enhanced reliable ant colony optimization routing in vehicular ad hoc networks," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, 2018, pp. 1071-1078.

[98] A. M. Vegni and T. D. C. Little, "A message propagation model for hybrid vehicular communication protocols," in *Proc. 7th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Newcastle Upon Tyne, U.K., 2010, pp. 382-386.

[99] S. M. Zin, N. B. Anuar, M. L. M. Kiah, and I. Ahmedy, "Survey of secure multipath routing protocols for WSNs," *J. Netw. Comput. Appl.*, Vol. 55, pp. 123-153, 2015.

[100] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," *J. Netw. Comput. Appl.*, vol. 33, no. 4, pp. 422-432, 2010.

[101] D. Han and J. M. Chung, "Self-similar traf_c end-to-end delay minimization multipath routing algorithm," *IEEE Commun. Lett.*, vol. 18, no. 12, pp. 2121-2124, 2014.

[102] Y. Challal, A. Ouadjaout, N. Lasla, M. Bagaa, and A. Hadjidj, "Secure and ef_cient disjoint multipath construction for fault tolerant routing in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 34, pp. 1380-1397, 2011.

[103] A. S. Lal and R. Nair, "Region authority based collaborative scheme to detect Sybil attacks in VANET" in *Proc. Int. Conf. Control Commun. Comput. India (ICCC)*, 2015, pp. 664-668.

[104] P . P. C. Lee, V. Misra, and D. Rubenstein, "Distributed algorithms for secure multipath routing in attack-resistant networks," *IEEE/ACM Trans. Netw.*, vol. 15, no. 6, pp. 1490-1501, 2007.

[105] Y . Cao, F. Song, Q. Liu, M. Huang, H. Wang, and I. You, "A LDDoS- Aware energy-efficient multipathing scheme for mobile cloud computing systems," *IEEE ACCESS*, vol. 5, pp. 21862-21872, 2017.

[106] P. M. Mohan, T. J. Lim, and M. Gurusamy, " Fragmentation-based multi-path routing for attack resilience in software defined networks," in *Proc.IEEE 41st Conf. Local Comput. Netw. (LCN)*, Dubai, UAE, 2016, pp. 583-586.

[107] M . Saad, A. Leon-Garcia, and W. Yu, "Optimal network rate allocation under end-to-end quality-of-service requirements," *IEEE Trans. Netw. Service Manage.*, vol. 4, no. 3, pp. 40_49, 2007.

[108] W. H. Wang, M. Palaniswami, and S. H. Low, "Application-oriented flow control: Fundamentals, algorithms and fairness," *IEEE/ACM Trans. Netw.*, vol. 14, no. 6, pp. 1282_1291, 2006.

[109] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, Vol. 10, no. 10, pp. 3528-3540, 2011.

[110] J. Jin, M. Palaniswami, and B. Krishnamachari, "Rate control for heterogeneous wireless sensor networks: Characterization, algorithms and performance," *Comput. Netw.*, vol. 56, pp. 3783-3794, 2012.

[111] N.J. Habeeb, S.T. Weli, Relationship of smart cities and smart tourism: an overview. *HighTech Innovat J*, Vol. 1 (4), pp. 194-202, 2020.

[112] M. Sichitiu, M. Kihl, "Inter-vehicle communication systems: A survey." *IEEE Communications Surveys & Tutorials*, Vol. 10(2), pp. 88-105, 2008.

[113] S. Tanzila, S. Tariq, R. Amjad, M. Zahid, and J. Qaisar, "Intrusion Detection System Through Advance Machine Learning for the Internet of Things Networks." *IT Professional*, Vol. 23(2), pp. 58-64, 2021.

[114] K. Gu, X. Dong, W. Jia, Malicious node detection scheme based on correlation of data and network toplogy in fog-computing based VANETs." *IEEE Transaction on Cloud Computing*, Vol. 5(2), pp. 1-18, 2020.

[115] R. Hussain, F. Hussain, S. Zeadally, "Integration of VANET and 5G security: A review of design and implementation issues." *Future generation computer systems*, Vol. 101(3), pp. 843-864, 2019.

[116] D. Manivannan, M. Shawkat, S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)." *Vehicular Communications*, Vol. 25(2), pp. 1-18, 2020.

[117] S. A. Siddique, A. Mahmood, Q.Z. Sheng, H. Suzuki, W. Ni, "A survey of trust management in the internet of vehicles," *Electronics*, Vol. 10, 2223, 2021.

[118] C. Huang, R. Lu, K.K.R. Choo, "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges." *IEEE Communications Magazine*, Vol. 55(11), pp. 105-111, 2017.

[119] M. Mukherjee, M. Matam, Shu, "Security and privacy in fog computing: Challenges." *IEEE Access, Vol.* 5, pp. 19293-19304, 2017.

[120] F. Bonomi, "Connected vehicles, the internet of things, and fog computing." *The eighth ACM international workshop on vehicular internetworking (VANET),* pp.13-15, 2011.

[121] A. Iftikhar, H.K Zawar, G. Aaron, S. Khurram, M.A.K. Khattak, M.A.K., A. Murtaza, M. Nasru. "Macroscopic Traffic Flow Characterization at Bottlenecks." *Civil Engineering Journal,* Vol. 6(7), pp. 1227–1242, 2020.

[122] G. Rehman, A. Ghani, M. Zubair, I. Saeed, D. Singh, "SOS: Socially omitting selfishness in IoT for smart and connected communities." *International Journal of communication systems,* Vol. 1(25), pp. 1-16, 2020.

[123] M. Hasan S. Mohan, T. Shimizu, H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms." *IEEE transactions on intelligent vehicles*, Vol. 25(1), pp. 1-22, 2020.

[124] M.V. De, R. Brundo, I. Brandic, Energy and profit aware proof-of-stake offloading in blockchain-based VANETs. *Proceedings of 12th IEEE/ACM international conference on utility and cloud computing UCC 19,* pp. 177-186, 2019.

[125] N.C. Velayudhan, A. Anitha, M. Madanan, V. Paul, "Review on avoiding Sybil in VANET while operating in an urban environment." *Journal of Theoretical and Applied Information Technology*, Vol. 97(20), 2019..

[126] A. Zouinkhi, A. Ltifi, C. Chouaib, M. Naceur, " A trust management based on cooperative scheme in VANET," *International Journal of Information and Communication Technology*, Vol.13 No.3, pp.291 - 304, 2012.

[127] R.W. Van-der-Heijden, F. Kargl, O.M. Abu-Sharkh, A. Al-Momani, "Enhanced position verification for vanets using subjective logic." *IEEE 84th Vehicular Technology Conference (VTC-Fall),* pp. 1-7, 2016.

[128] A. Rrecaj, V. Alimehaj, M. Malenkovska, C. Mitrovski, "An Improved CTM model for urban signalized intersections and exploration of traffic evaluation." *Civil Engineering Journal*, Vol. 7(2), pp. 357-375, 2021.

[129] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A robust and privacy-preserving reputation management scheme for pseudonym enabled VANETs," *Int. J. Distrib. Sensor Netw.*, vol. 1(16), Art. no. 6138251, 2016.

[130] U . F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular

networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407-420, 2011.

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

[132] D. B. Rawat, B. 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, 2011, pp. 146-151.

[133] O . A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on Dempster-Shafer for detecting misbehaving vehicles," *Comput. Commun.*, vol. 41, pp. 43-54, 2014.

[134] A. El Khatib, A. Mourad, H. Otrok, O. A. Wahab, and J. Bentahar, "A cooperative detection model based on artificial neural network for VANET QoS-OLSR protocol," in proc. *IEEE ICUWB*, Montreal, QC, Canada, 2015, pp. 1-5.

[135] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM based intelligent detection model for clustered vehicular ad hoc networks," *Expert Syst. Appl.*, vol. 50, pp. 40-54, 2016.

[136] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen, C. Sun, "DAPV: Diagnosing Anomalies in MANETs Routing With Provenance and Verification," *IEEE Access,* Vol. 7, pp. 35302–35316, 2019.

[137] J. Wilson,K. Subramaniam, "Improved multi objective data transmission using conventional route selection algorithm in mobile ad hoc network," *Peer-to-Peer Networking and Applications*, Vol. 13, pp. 1091–1101 2020.

[138] S. Du, J. Hou, S. Song, Y. Song, Y. Zhu, "A geographical hierarchy greedy routing strategy for vehicular big data communications over millimeter wave," *Physical Communication*, Vol. 40, pp. 1–9, 2020.

[139] W. Fang, W. Zhang, W. Chen, Y. Liu, C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Networks*, Vol. 26, pp. 3169–3182 2020.

[140] T.K. Saini, S.C. Sharma, "Recent advancements, review analysis, and extensions of the aodv with the illustration of the applied concept," *Ad Hoc Networks*, Vol. 103, pp. 1–20, 2020.

[141] H. Kojima, N. Yanai, J.P. Cruz, "ISDSRC: Improving the security and availability of secure routing protocol," *IEEE Access* Vol. 7, pp. 74849–74868, 2019.

[142] Y. Park, C. Sur, K.H. Rhee, "A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency," *Security and Communication Network*, Vol. 18, pp. 1-13, 2018.

[143] A. Sharma, E.S. Pilli, A.P. Mazumdar, P. Gera, "Towards trustworthy internet of things: A survey on trust management applications and schemes," *Computer Communications*, Vol. 160, pp. 475–493, 2020.

[144] R.K. Chahal, N. Kumar, S. Batra, "Trust management in social internet of things: A taxonomy, open issues, and challenges," *Computer Communications*, Vol. 150, pp. 13–46. 2020.

[145] R.J. Cai, X.J. Li, P.H.J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," *IEEE Transactions on Mobile Computing*, Vol. 18(1), pp. 42–55, 2019.

[146] S.N. Mahapatra, B.K. Singh, V. Kumar, "A survey on secure transmission in internet of things: Taxonomy, recent techniques, research requirements, and challenges," *Arabian Journal for Science and Engineering*, Vol. 45, pp. 6211–6240, 2020.

[147] M.A. Qurashi, C.M. Angelopoulos, V. Katos, "An architecture for resilient intrusion detection in ad-hoc networks," *Journal of Information Security and Applications*, Vol. 53, pp. 1–12, 2020.

[148] H. Riasudheen, H., K. Selvamani, S. Mukherjee, M. Divyasree, "An efficient energy-aware routing scheme for cloud-assisted manets in 5G," *Ad Hoc Networks*, Vol. 97, pp. 1–22, 2020.

[149] H. Xu, et al "Trust-based probabilistic broadcast scheme for mobile ad hoc networks," *IEEE Access*, Vol. 8, pp. 21380–21392, 2020.

[150] P. Theerthagiri, "FUCEM: futuristic cooperation evaluation model using markov process for evaluating node reliability and link stability in mobile ad hoc network," *Wireless Networks*, Vol. 26, pp. 4173–4188, 2020.

[151] N. Djedjig, D. Tandjaoui, F. Medjek, I. Romdhani, "Trust-aware and cooperative routing protocol for iot security," *Journal of Information Security and Applications*, Vol. 52, pp. 1–17, 2020.

[152] R.H. Jhaveri, N.M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," *International Journal of Communication Systems*, Vol. 30, pp. 1–24, 2016.

[153] A.M. Desai, R.H. Jhaveri, "Secure routing in mobile Ad hoc networks: a predictive approach," *International Journal of Information Technology volume*, Vol. 11, pp. 345–356, 2018.

[154] R.H. Jhaveri, A. Desai, A. Patel, Y. Zhong, "A Sequence Number Prediction Based Bait Detection Scheme to Mitigate Sequence Number Attacks in MANETs," *Security and Communication Networks, Wiley-Hindawi*, 1–13, 2018.

[155] L. Chen, Q. Li, K. M. Martin, "Private reputation retrieval in public-a privacy-aware announcement scheme for VANETs," *IET Inf. Secur.* Vol. 11(4), pp. 204–210, 2016.

[156] Z. Lu, Q. Wang, G. Qu, Z. Liu, "BARS: a blockchain-based anonymous reputation system for trust management in VANETs" in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)., IEEE, New York*, pp. 98–103, 2018.

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

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

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

[160] 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.

[161] 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.

[162] R. Sun, Y. Huang, L. Zhu, "Communication by Credence Credit based: Trust Communication in Vehicular Ad Hoc Networks," *Mobile Netw Appl.*, Vol. 71, pp. 1-13, 2021.

[163] P. Sankar, A. Kumar, B. Bharathi. "Blockchain-Based Incentive Announcement In Vanet Using CreditCoin". *Advances in Electronics, Communication and Computing.*, Vol. 709. pp. 567-574, 2021.

[164] 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.

[165] L. Alouache, N. Nguyen, M. Aliouat, R. Chelouah, "Credit Based Incentive Approach for V2V Cooperation in Vehicular Cloud Computing," *Internet of Vehicles*, Vol. 11253, 2018.

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

[167] G. Zhao, M. Chen, X. Wei, "RIS: A reciprocal incentive scheme in selfish opportunistic networks," *Wirel. Pers. Commun.*, Vol. 70, pp. 1711–1734, 2013.

[168] H. Liu, P.C Lee, J.C.S. Lui, "On the credit evolution of credit-based incentive protocols in wireless mesh networks," *Comput. Netw.*, Vol. 57, pp. 3327–3343, 2013.

[169] T. Seregina, O. Brun, R. El-Azouzi, B.J. Prabhu, "On the design of a reward-based incentive mechanism for delay tolerant networks," *IEEE Trans. Mob. Comput.* Vol. 16, pp. 453–465, 2017.

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

[171] J. Li, X.Wang, R. Yu, "Reputation-based incentives for data dissemination in mobile participatory sensing networks,"*Int. J. Distrib. Sens. Netw.* Vol.11, pp. 172130, 2015.

[172] A. Katmada, A. Satsiou, I. Kompatsiaris, "A reputation-based incentive mechanism for a crowdsourcing platform for financial awareness,"In Proc. *International Workshop on the Internet for Financial Collective Awareness and Intelligence (IFIN 2016),* Florence, Italy, pp. 57–80, 2016.

[173] Y. Zhan, Y. Xia, J. Zhang, Y. Wang, "Incentive mechanism design in mobile opportunistic data collection with time sensitivity," *IEEE Int. Things J.*, Vol. 5, pp. 246–256, 2018.

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

[175] M. Louta, P. Bellavista, "Bringing always best connectivity vision a step closer: challenges and perspectives," *IEEE Commun. Mag.*, Vol. 51 (2), pp. 158–166, 2013.

[176] P. Resnick, K. Kuwabara, R. Zeckhauser, *et al.* "Reputation systems," *Commun. ACM*, Vol. 43(12), pp. 45–48, 2000.

[177] G. Dini, A.L Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network," *Ad Hoc Netw.*, Vol. 10(7), pp. 1167–1178, 2012.

[178] R. Chen, F. Bao, M. Chang, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distrib. Syst.*, Vol. 25(5), pp. 1200–1210, 2014.

[179] Y. Zhu, B. Xu, X. Shi, X, "A survey of social-based routing in delay tolerant networks: positive and negative social effects," *IEEE Commun. Surv. Tutor.*, Vol. 15(1), pp. 387–401, 2013.

[180] N. Chakchouk, "A survey on opportunistic routing in wireless communication networks," *IEEE Commun. Surv. Tutor.*, Vol. 17(4), pp. 2214–2241, 2015.

[181] S. Kraounakis, I.N. Demetropoulos, A. Michalas,"A robust reputation-based computational model for trust establishment in pervasive systems," *IEEE Syst. J.*, Vol. 9(3), pp. 878–891, 2015.

[182] X. Li, F. Zhou, X. Yang, "Scalable feedback aggregating (sfa) overlay for large-scale p2p trust management," *IEEE Trans. Parallel Distrib. Syst.*, Vol. 23(10), pp. 1944–1957, 2012.

[183] M. Eirinaki, M.D. Louta, I. Varlamis, "A trust-aware system for personalized user recommendations in social networks," *IEEE Trans. Syst. Man Cybern., Syst.*, Vol. 44(4), pp. 409–421, 2014.

[184] I. Varlamis, M. Eirinaki, M. Louta, "Application of social network metrics to a trust-aware collaborative model for generating personalized user recommendations," *Influence Technol. Social Netw. Anal. Mining*, Vol. 6, pp. 49–74, 2013.

[185] G. Zhan, W. Shi, J. Deng, "Design and implementation of tarf: a trust-aware routing framework for wsns', *IEEE Trans. Dependable Secur. Comput.*, Vol. 9(2), pp. 184–197, 2012.

[186] S. Bera, S. Misra, S.K. Roy, "Softwsn: software-defined wsn management system for iot applications," *IEEE Syst. J.*, Vol. PP(99), pp. 1–8, 2016.

[187] S. Sicari, A. Rizzardi, L.A. Grieco, "Security, privacy and trust in internet of things: the road ahea," *Comput. Netw.*, Vol. 76, pp. 146–164, 2015.

[188] S. Ruohomaa, L. Kutvonen, "Trust management survey," '*ITrust*' Vol. 3477, pp. 77–92, 2005.

[189] S. Trifunovic, F. Legendre, "Trust in opportunistic networks," *Comput. Eng. Netw. Lab.*, pp. 1–12, 2009.

[190] K. Wei, X. Liang, K. Xu, "A survey of social-aware routing protocols in delay tolerant networks: applications, taxonomy and design-related issues," *IEEE Commun. Surv. Tutor.*, Vol. 16, (1), pp. 556–578, 2014.

[191] W. Moreira, P. Mendes, "Social-aware opportunistic routing: the new trend," *Routing in Opportunistic Networks*' Springer, pp. 27–68, 2013.

[192] K. Hoffman, D. Zage, C. Nita-Rotaru,"A survey of attack and defense techniques for reputation systems," *ACM Comput. Surv. (CSUR)*, Vol. 42 (1), p. 1-13, 2009.

[193] R. Kerr, R. Cohen, "Smart cheaters do prosper: defeating trust and reputation systems," In Proc. of the *8th Int. Conf. Autonomous Agents and Multiagent Systems-Volume 2. Int. Foundation for Autonomous Agents and Multiagent Systems*, 2009, pp. 993–1000.

[194] A. Josang, J. Golbeck, "Challenges for robust trust and reputation systems," in Proc. of the *5th Intl. Workshop on Security and Trust Management (SMT 2009)*, Saint Malo, France, 2009, pp. 52-62.

[195] Q. Jiang, C. Men, H. Yu, "A secure credit-based incentive scheme for opportunistic networks," in Proc. *7th Int. Conf. Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, 2015, vol. 1, pp. 87–91.

[196] A. Sharma, "A credit based routing mechanism to contrast selfish nodes in delay tolerant networks," in Proc. *Int. Conf. Parallel, Distributed and Grid Computing (PDGC)*, 2014, pp. 295–300.

[197] A. Jesudoss, S.V. Kasmir, A. Sulaiman "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme" *Ad Hoc Networks*, Vol. 24, pp. 250–263, 2015.

[198] R.P.Nayak, S. Sethi, S.K. Bhoi, et al. "ML-MDS: Machine Learning based Misbehavior Detection System for Cognitive Software-defined Multimedia VANETs (CSDMV) in smart cities" *Multimed Tools Appl.* pp. 35-41, 2022.

[199] M. M. Hamdi, M. Dhafer, A. S. Mustafa, S. A. Rashid, A. J. Ahmed and A. M. Shantaf, "Effect Sybil attack on security Authentication Service in VANET," in Proc. *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-6, 2022.