Article

Not peer-reviewed version

Improved Authentication and Communication Schemes for Urban Traffic Monitoring in VANETs Based on Cluster Management

Rana Muhammad Amir Latif , Muhammad Jamil , Jinliao He * , Muhammad Farhan

Posted Date: 10 May 2023

doi: 10.20944/preprints202305.0683.v1

Keywords: Traffic Monitoring; Intelligent Transportation System; VANETs, Cluster-Based Routing Scheme; P2P Wireless Communications

Article

Improved Authentication and Communication Schemes for Urban Traffic Monitoring in VANETs Based on Cluster Management

Rana Muhammad Amir Latif [1], Muhammad Jamil [2], Jinliao He [1,*] and Muhammad Farhan [2]

[1] The Center for Modern Chinese City Studies, Institute of Urban Development, East China Normal University, Shanghai 200062, China; 52263902018@stu.ecnu.edu.cn

[2] Department of Computer Science COMSATS University Islamabad, Sahiwal Campus Sahiwal, Pakistan; jamil138.amin@gmail.com (M.J.); farhansajid@gmail.com (M.F.)

* Correspondence: jlhe@iud.ecnu.edu.cn

Abstract: City zones have become increasingly overcrowded as a result of the extensive population widening ratio and the swift relocation of people from villages. The traffic monitoring process is a major issue in these areas due to the massive traffic flow on the roads. This research proposed a cluster-based improved authentication and communication scheme for an Intelligent Transportation System in Vehicular AdHoc Networks (VANETs). Our primary objective is to optimize resource sharing in vehicular communication. We enhanced the reliability, scalability, and stability of fast-moving VANETs by introducing cluster-based routing schemes for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. We used a third-party certification authority for vehicle authentication to address security and privacy concerns. Our proposed schemes support minimizing the end-to-end (E2E) delay and route request, in addition to reducing link failure. Our schemes' leading yield includes throughput enhancement, TCP Socket Initialization time minimization, TCP handshake response speedup, and DNS lookup improvement. The schemes are centred on short-range peer-to-peer (P2P) wireless communication in a 400-meter radius cluster. This includes innovative P2P wireless communications on VANET using minimized resources. The proposed schemes deliver a secure authentication mechanism with a securely generated vehicle authentication key provided by a certification authority. Furthermore, we have developed RESTful APIs in vehicular communication for implementation purposes, and also offered and implemented algorithms for resource sharing regarding V2V and V2I communication. Ultimately, we evaluated the performance of our experiments.

Keywords: traffic monitoring; intelligent transportation system; VANETs; cluster-based routing scheme; P2P wireless communications

1. Introduction

The rapid migration of people from villages to cities has produced major threats in regard to controlling the overfilled traffic. Traffic congestion in a city environment has now become the focal point of many researchers. Vehicular AdHoc networks provide the Intelligent Transportation System with the help of Road Side Units (RSU). These networks are the primary source of improving driving safety by decreasing roadside accidents [1]. However, RSU message passing is categorized under Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communication. VANETs help minimize roadside accidents and recognize the positions of vehicles moving along the same track. On VANETs, spotting emergency vehicles, such as patrol cars and ambulances, is an easy task. This process is subject to acquiring the moving vehicle's actual location. According to the authors [2], location service is the critical application of VANETs. There is a belief that Intelligent Transportation Systems employ the Internet of Everything (IoE). The authors' paper also discusses monitoring the traffic flow using edge computing in VANETs [3]. Resource sharing is one of the significant issues involved with vehicular communication. Resource sharing in high-vehicle mobility requires significant power consumption; which is a severe obstacle in vehicular Communication [4]. To optimize resource utilization and reduce network signal overhead, distributed resource management is beneficial [5].

P2P (Peer-to-Peer) systems using a wireless network are growing in popularity due to the evolution of the internet. These systems provide optimal performance while sharing messages and other resources. Road safety applications using P2P wireless networks are also becoming a vital part of the VANET for traffic monitoring [6,7]. For Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), the area is selected by determining a particular cluster, or through a distance radius. An Intelligent Traffic System brings about numerous benefits to traffic management [8]. These benefits include on-the-mark traffic monitoring, right traffic congestion analysis, sending accurate traffic violation warnings to drivers, traffic infrastructure analysis, and sending messages using V2V and V2I Communication [9].

In an ITS, the average message response time typically takes up to 10 times in milliseconds. The cluster or a distance radius usually has a radius range of approximately 400 meters. On a Vehicular AdHoc Network, the message passing can be done through textual, graphic, and audible information. The VANET must be secured against cyber-attacks, unauthorized access, identity theft, and phishing [10]. It may be stated that VANET security is breached when someone gains unauthorized access to a particular Vehicle Onboard Unit (OBU), and is able to alter or hinder the vehicle's main functionality. Due to traffic congestion or bad road infrastructure, there is a chance of vehicle collision [11]. The "Crash Possibility" message can be conveyed to the vehicle in an attempt to overcome this issue. Distance measurement is a necessary element to generate a collision warning message; which can be performed using a camera and a sensor [12]. There is a problem of false messages passing for vehicle collision warnings. To eliminate this issue, we took the services of a third-party Certification Authority. The CA will carry out multiple functions like vehicle registration and vehicle authentication. It also acts as a bridge for V2V and V2I communications. Due to authentication with CA, the identity of the false message sender can be highlighted as shown in Table 1.

Table 1. Indexed Terms Meanings.

Keyword	Meanings
ITS	Intelligent Transportation System
VANETs	Vehicular AdHoc Networks
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2X	Vehicle-to-Everything
RSU	Road Side Units
E2E	End-to-End
PDR	Packet Delivery Ratio
RR	Route Reliability
P2P	Peer-to-Peer
TRPs	Topological Routing Protocols
GRPs	Geographic Routing Protocols
5G	Fifth Generation
SDN	Software-Defined Network
DDoS	Distributed Denial of Services
MANETs	Mobile AdHoc Networks
CA	Certification Authority

LCG	Linear Congruential Generator
FYS	Fisher-Yates Shuffle
API	Application Programming Interface
OTP	One-Time Password
HTTP	Hypertext Transfer Protocol
UR	Ultra-Reliability
IoT	Internet of Things
AI	Artificial Intelligence
MD5	Media-Digest Algorithm for encryption
SUMO	Simulation of Urban Mobility
API	Application Program Interface
TCP	Transfer Control Protocol

We proposed secure cluster-based authentication and communication schemes for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. Our work covers the following phases for V2I and V2V communications and resource sharing in a VANET.

- Authentication and registration using third-party Certification Authority
- V2I & V2I Communication Channel
- Graph-Based Resource Sharing in Vehicular Communication

For registration and authentication, we took up assistance from the third-party Certification Authority. We demonstrated the V2V and V2I communication mechanism in a 400-meter diameter. We addressed primary security goals like integrity, authenticity, and availability of messages in vehicular communication on a specific cluster. Figure 1 simplifies the Vehicle-to-Vehicle communication in a 400-meter cluster. CH means the Head of the Cluster, and CM denotes the other Cluster Member. We proposed two algorithms based on baseline and greedy approaches for resource allocation in vehicular communications.

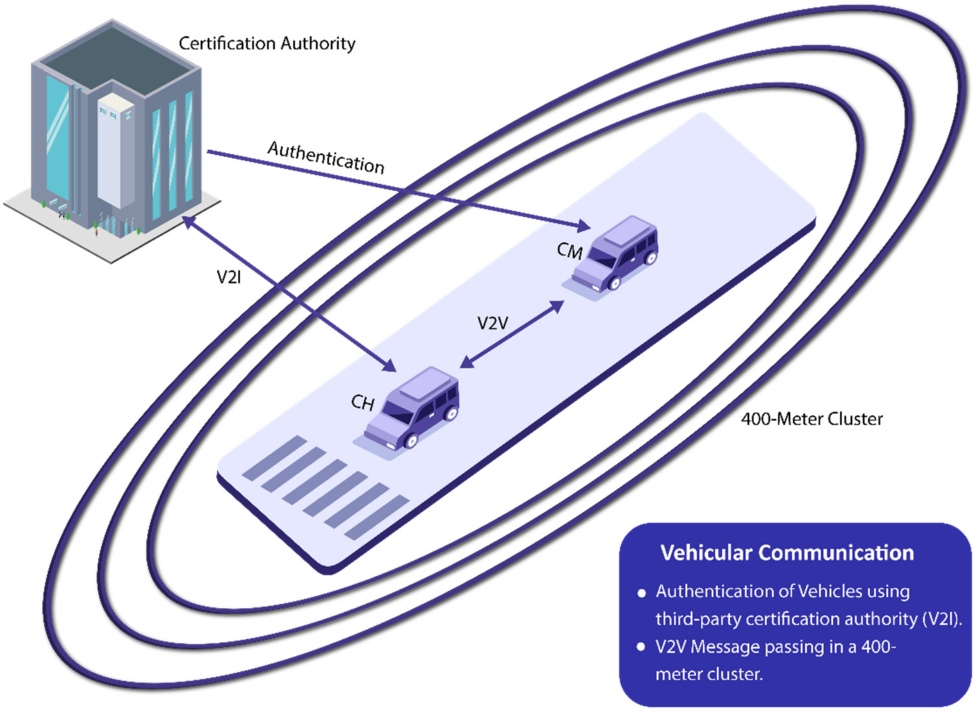
Certification Authority
Authentication
V2I
CM
V2V
CH
400-Meter Cluster
Vehicular Communication
• Authentication of Vehicles using third-party certification authority (V2I).
• V2V Message passing in a 400-meter cluster.

Figure 1. Vehicular communication in a 400-meter diameter.

Section 1 addresses the introduction and research contribution. In Section 2, we have discussed previous studies relevant to the research. We compared the various past research contributions on VANET with the aid of a comparison table. Section 3 includes the research methodology, implementation, performance evaluation, results, and discussions. The methodology section includes the demonstration of the proposed scheme, implementation, and graph-based resource sharing in vehicular communications. This section further addresses notations and assumptions, research results, and performance evaluation. In the implementation subsection, we have discussed the utilized tools and technologies. Ultimately, we have concluded our research in the conclusion section.

2. Literature Review

In VANETs, the significant contribution of the researchers includes (a) a central service directory architecture [13–15], (b) directory-less service architecture [16–18], and (c) distributed directory service architecture [19–23]. In the first portion, based on central service discovery architecture, the researchers proposed a central discovery server to store the service information and re-join a discovery request with the matched discovery outcomes. Ali et al. [13] discussed a three-way link between 5G technology, Software-Defined Networks, and Vehicular AdHoc Networks. The authors concentrated on creating a network balance through highlighting the mobility, security, and performance of software-defined networks (SDN). The authors of [14] discussed mystery location-oriented and self-reliance protocols for Mobile AdHoc Networks routing. The authors anticipated their views on a secure packet delivery mechanism in MANETs for vehicular communications. Edge et al. [15] discussed the techniques and methods for providing location-based services for users' tools by requiring assistance from Service-Based Interfaces.

The authors [17] proposed the idea of edge computing in Vehicular AdHoc Networks using bit-blocking protocol infrastructure. The authors [18] elucidated the use and function of wireless Vehicular AdHoc Networks. They differentiated the structure of MANETs and Cellular Networks. Yang et al. [19] clarified the Vehicle-to-Vehicle (V2V) communications using Peer-to-Peer networks through employing graph theory and consensus algorithm. The authors omitted the Roadside Units and defined the serial communication between vehicles moving along the road. The authors [20] conducted three focus group interviews and eight individual interviews to address trust and privacy matters in Peer-to-Peer networks. Shah et al. [21] provided a visual paradigm of VANET in a 5G technology-based network. The authors [22] described the concept of vehicular cloud by using P2P routing protocols to prevent road accidents, monitor traffic, and ensure fast content delivery. Singh et al. [23] wrote a survey paper on the state of the art vehicular communications and future directions for further studies. Salem et al. [24] proposed a self-organized framework for VANETs. They applied mathematical analysis to their proposed framework in order to enhance security goals. They also evaluated their framework's performance in terms of computation complexity, storage, and communication overhead. By comparing several schemes, they also tested their framework against several types of external attacks. The authors of [25,26] evaluated the performance of vehicular communication on P2P wireless network, while the authors of [27–30] discussed several security issues and challenges in VANETs with multiple dimensions including P2P wireless networks. Table 2 consists of the comparison of previous research over vehicular communication and VANETs, while Figure 2 displays various VANET routing protocols.

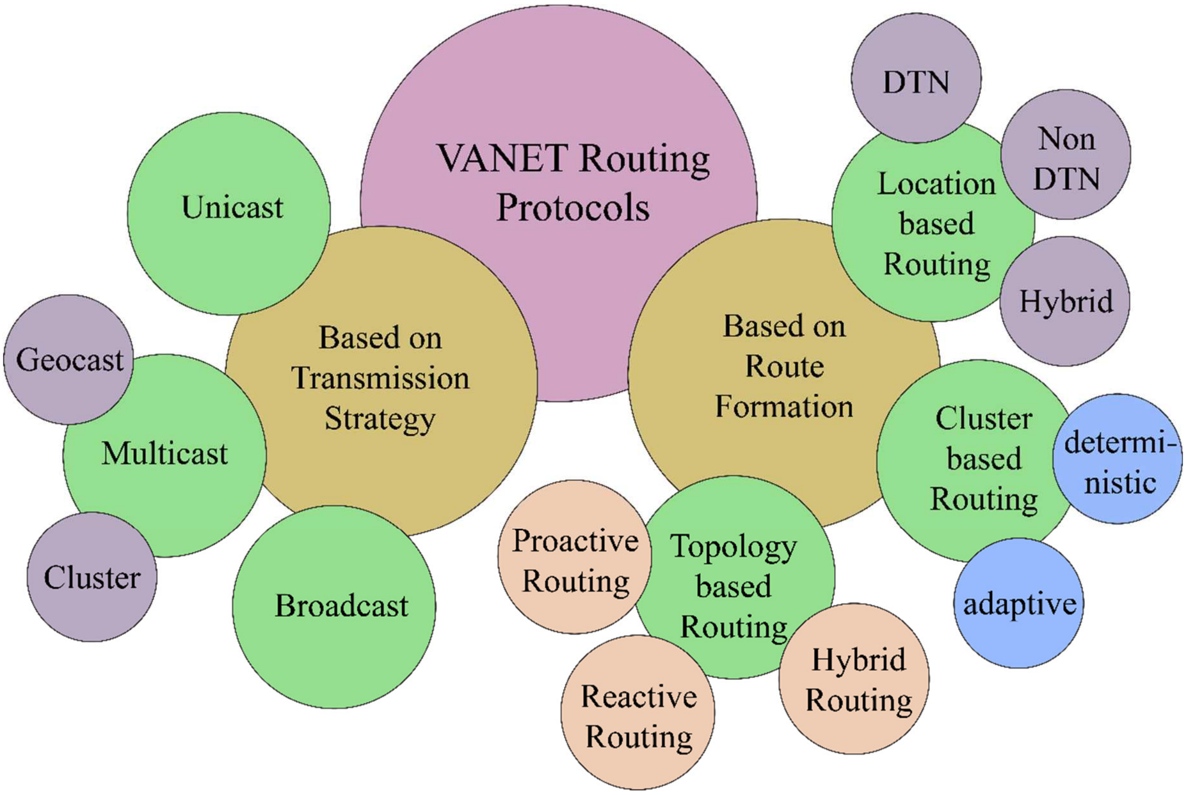

Figure 2. VANET Routing Protocols.

Table 2. compares related works on Vehicular Communication with paper reference, publishing year, and significant contribution attributes. (✓) indicates that the topic is covered completely, whereas (✗) means no discussion is present, and (✻) conveys that the topic is covered partially.

Table 2. Related Work Comparison.

Ref No.	Key Contribution	V2V	V2X
[31]	• AI transmission scheduling in cognitive vehicular communication • Vehicular communication modes	✓	✓
[32]	• Resource allocation and power-sharing with several optimal resource allocation algorithms	✓	✓
[33]	• Mobile edge computing framework • Network paradigm with predictive off-loading	✓	✓
[34]	• Hierarchy of wireless networks and network standards • cumulative smart grid model • IoT security analysis	✻	✻
[35]	• Models and communication channel measurement metrics for wireless infrared networks	✻	✻
[36]	• Longitudinal safety assessment of connected vehicles • Intelligent driver model in a connected vehicle network	✓	✻
[37]	• Survey V2V-based vehicular sensor networks communications • Issues and challenges in V2C communication	✓	✻

[38]	• A physical layer perspective of vehicular communications	✻	✓
[39]	• A short-range model for Vehicle-to-vehicle communication on Vehicular AdHoc Networks through • The showcase of Vehicle-to-Vehicle communication probability analysis	✓	✗
[40]	• A hybrid clustering algorithm • Simulation of the proposed algorithm on SUMO	✻	✻
[41]	• A distributed Cloud structure for urban traffic management through a cloud service handled message algorithm	✻	✻
[42]	• Implementation of the Markov renewal process • Classification of message passing between Road Side Units and Vehicles	✻	✓
[43]	• Proposed a Cell Transmission Model for expressway traffic	✻	✓
[44]	• Proposed a distributed cloud-based architecture for Vehicular AdHoc Networks performance • An additional mathematical model for strong communication of vehicles	✗	✓
[42]	• A secure communication scheme for Vehicular AdHoc Networks	✓	✓
[45]	• It highlighted the difficulties in implementing VANET systems due to traffic, communication, and safety concerns, and it investigated how machine learning techniques may help address these challenges.	✓	✓
[46]	• To maximize global criteria while simultaneously boosting class longevity, information transmission speed, and lowering inter-class overload. • We provide an Efficient Key Management Scheme (KMSUNET) based on symmetric and asymmetric encryption to solve the performance and security issues of the UVANET environment.	✓	✻
[47]	• The suggested approach aims to establish reliable and steady clusters contributing to the network's overall reliability.	✓	✓
[48]	• Over time, the percentage of malicious nodes in a vehicle AdHoc network may be reduced thanks to this scheme's capability to identify and remove them.	✓	✻
[49]	• A novel self-adaptive Angular-based k-medoid Clustering Algorithm (SAACS) is created to generate flexible clusters. The network latency decrease and clusters are built using informed predictions about route lengths and signal ranges.	✓	✓
[50]	• To provide a comprehensive summary of the many methods currently being considered in the literature as potential solutions to the issue of traffic congestion.	✓	✻

[51]	• Scholars are now more responsible for safeguarding individuals' private data and information. • Puts forward the Key Agreement Protocol for Urbanized Block Chains (UB-KAP)	✓	✻
[52]	• An innovative REST web service for visualizing data is proposed. • The Fundamental Safety Messages were put through their paces in a Big Data lab. • Proper behaviour concerning packet loss, packet delivery, and communication latency was shown.	✓	✓
[53]	• For this reason, the AWCP EE-WOA model analysis includes a vehicular network at a predetermined velocity and location.	✓	✻

Routing protocols play an essential role in vehicular AdHoc networks; expediting the provision of several services through facilitating the transmission of messages from one node to another. There are two distinct categories for VANET routing protocols. Topological Routing Protocols (TRPs) are one kind, while Geographic Routing Protocols (GRPs) are another. Topological routing protocols maintain data links and disseminate topological data. Scalability issues, time- consumption discovery, cumbersome control requirements, and tedious maintenance are merely a number of the challenges that TRPs must overcome.

On the other hand, Geographic Routing Protocols depend on the most up-to-date location information to establish connections with moving vehicles. Keeping and disseminating the connection data is optional. Because of their simplicity and low overhead, these protocols function well in highly dynamic, large-scale networks. Compared to topological routing protocols, geographical routing protocols perform and scale better, while having a lower routing overhead. Obtaining the precise coordinates of the vehicles, and then adjusting the routes accordingly is a necessary first step in developing GRPs [54–58]. Figure 3 provides the hierarchy of routing protocols with their significant components.

Zhang et al. [31] presented a brief account of Artificial Intelligence Transmission Scheduling in cognitive vehicular communications and networks. They discussed several vehicular communication modes, including V2V and V2I. They also investigated the features of these communication modes and spectrum resources adopted by vehicles in diverse network states with numeric values. As a result, they proposed a deep reinforcement earning algorithm for optimal scheduling of vehicular communication. Liang et al. [32] discussed resource allocation and power-sharing in vehicular communication. They debated the requirements for different links, like high capacity for V2I links and UR for V2V links. They proposed several optimal resource allocation algorithms for better resource allocation and power-sharing. Zhang et al. [33] discussed a capable network paradigm with predictive off-loading for vehicular networks. The authors explained the cloud-based vehicular networks in multiple dimensions by proposing a mobile edge computing framework. They talked about the effectiveness of V2V and V2I communication modes in terms of vehicle mobility, and time consumption of executing the computation task. The authors of [34] discuss the hierarchy of various types of wireless networks and network standards. They examine a cumulative smart grid model for vehicle mobility and other wireless technologies. Furthermore, they have presented an overview of radio technologies with their corresponding ranges and IoT security analysis.

The authors [35] proposed several models and communication channel measurement metrics for wireless infrared networks. Their research discussed almost 20 optical wireless communication models with different communication scenarios. Rahman et al. [36] elaborated on the longitudinal safety assessment of connected vehicles moving on superhighways. They expressed their intelligent driver model in a connected vehicle network with a high-level control algorithm. They proposed three joining categories, including front join, rear join, and cut join, with possible safety measures such as time-to-collision, rear-end crash risk index, and sideswipe crash risk. Masini et al. [37] authored a survey paper on V2V-based vehicular sensor network communications. They discussed both V2V and V2X in the sense of visible light communication and 5G. They also discussed the challenges and issues posed by short-range V2V communication. The authors [38] discussed V2X channel models for communication by explaining the physical layer perspectives. The authors also discussed the resource allocation and challenges in vehicular communications.

Yan et al. [39] discussed Vehicle-to-Vehicle communication in Vehicular AdHoc Networks by introducing a short-range communication model. The authors also highlighted the probability analysis of Vehicle-to-Vehicle linking in road sections. Liu et al. [40] designed a modified clustering algorithm by modifying the improved force-directed algorithm and spectral-clustering algorithm. They utilized the SUMO tool to perform their experiments for cluster stability in VANETs. The authors of [41] described VANETs cloud architecture for traffic management using a cloud communication vehicle. They proposed a cloud service and vehicle handle message algorithms for V2V and V2V communication. [42] analyzed the message propagation speed in VANETs. They applied the Markov renewal process to categorize message passing between RSUs.

Xiao et al. [43] proposed a cell transmission model for freeway traffic on VANETs, and performed a thorough connection probability analysis. The authors also performed numerical simulations of their results with the help of different graphs. The authors (Ali et al., 2020) proposed a distributed architecture for VANET's performance based on fog technology. To ensure transmission reliability, they also developed a mathematical model for assertive communication between vehicles and the fog layer. In their research, the authors evaluated the performance of their proposed architecture by considering major factors like throughput, jitter, and delay time. The authors [42,59] proposed a privacy-preserving communication scheme for VANETs. They intermixed elliptic curve cryptography and an identity-based encryption scheme to compose their scheme. The authors addressed server impersonation, replay, modification, and man-in-middle attacks.

Various researchers such as [60] have proposed models regarding cluster-based routing in VANETs, and a stream position performance analysis methodology was presented to address security concerns. Their model is based on DDoS attack detection and uses various factors that become a source of threat to cluster-based routing. The authors [61] used a real geographic scenario to analyze the cluster-based routing protocol for VANET. They simulated their work on SUMO for varying numbers of vehicles. By highlighting cluster-based routing protocol, the authors [62] discussed the applicability of a routing protocol on VANET. The authors [63] discussed the issues and challenges of location-based routing protocols in VANET. They also discussed the issues and challenges of cluster-based routing protocols.

The Vehicular AdHoc Network (VANET) is an Intelligent Transportation System (ITS) that requires regular monitoring for optimum operation. The goal of a VANET is successfully implemented via the application of Machine Learning algorithms; which allow the system to automatically learn from its data processing history and optimize itself accordingly. This article examines the safety, communication, and traffic-related challenges in VANET systems and how machine-learning methods may solve these issues. It also includes a case study demonstrating a VANET-based situation [45], and discusses future directions and obstacles.

In this study, we have addressed a multi-objective optimization problem to fine-tune the settings of a graph-based attribute-vector classification system (GCMAV). It seeks to optimize global criteria while increasing the class lifespan and the pace of information transmission and decreasing inter-class overload. It presents an Efficient Key Management Scheme (KMSUNET) that uses symmetric and asymmetric encryption to solve performance and security issues. The NetSim simulator and the MOEA framework were employes to run the simulations and fine-tune the settings. Open Street Map was used for the experiments' realistic maps, and the findings were compared to competing algorithms. The suggested technique performs well because of the typical inter-class lifespan and information transmission rate [46].

Vehicle-to-Vehicle communication and other cars, roadside devices, and infrastructure are made possible via Vehicular AdHoc Networks (VANETs); a special case of mobile AdHoc networks. Messages must be sent safely and reliably to increase security, facilitate the management of urban and road traffic, and offer services to the commuting public. This study presents a trust-based authentication mechanism for clustered vehicular AdHoc networks to build reliable and stable clusters, ensuring the stability of the entire whole. Cluster Heads (CHs) are chosen according to the predicted trust degree of each vehicle; which is calculated by adding the trust between cars and the trust between the vehicle and Road Side Units (RSUs). After being digitally signed by the sender, messages are encrypted using a public/private key-pair provided by a Trusted Authority (TA), and then decoded at the receiving end. Simulated results demonstrate that the suggested strategy improves malicious node detection accuracy, improves packet delivery ratio, and reduces authentication latency and overhead [47].

In terms of improving road safety and management, intelligent transportation systems, of which vehicular AdHoc networks are a crucial component, cannot be overstated. Nodes may be unable to obtain reliable traffic data if unscrupulous users insert phoney emergency warnings into the networks. In this paper, we offer a novel method for identifying malicious nodes that uses a fuzzy logic model to rate the reliability of each node. The vehicles are organized into groups, and an off-road device verifies the reliability of each node prior to allowing them access to the networks. Validation and demonstration of the technique's capability to identify and remove all malicious nodes over time are shown via simulations, decreasing the percentage of harmful nodes and raising the success rate of the supplied data [48].

This work offers a unique self-adaptable Angular-based k-medoid Clustering Scheme (SAACS) to create adaptable clusters. To decrease network latency, clusters are built by making educated assumptions about route lengths and signal ranges. A unique performance indicator, the cosine-based node uncoupling frequency, determines which will serve as the Cluster Head (CH). The parametric analysis range depends on the number of vehicular nodes that may receive a signal. Comparing the suggested method to others, such as Cluster Head Lifetime (CHL), Cluster Member Lifetime (CML), Cluster Number (CL), Cluster Overhead (CO), Packet Loss Ratio (PLR), and Average Packet Delay (APD), the experimental findings indicate that the proposed method provides superior service (APD). CML is 50% more effective than RTVC plus ECHS; whereas CHL is improved by 40% compared to RTVC alone. The suggested methodology reduces the ratio of lost packets to total packets, and the overhead incurred by other methods by 45%. As a result, the disparity between highway nodes in congested and sparse areas has shrunk [49]. The purpose of this research is to give a comprehensive analysis of the solutions presented so far to alleviate traffic congestion. It covers and analyses the three major subsystems of a Traffic Management System, and offers and discusses future research directions and notable topics that require additional examination for a practical and effective Traffic Management System [50].

This study suggests employing a one-way hash chain model based Urbanized Block Chain Key Agreement Protocol (UB-KAP) to strengthen privacy and data integrity safeguards in VANET-based healthcare networks. To expedite replies, beacons use a packet classification procedure to identify which emergency messages are safe and which are dangerous. To ensure the effectiveness of the proposed model, SUMO simulates road traffic (Simulation of Urban Mobility). The overall assessment considers the data collected per user, the message delivery ratio, the total data acquired, the latency, and the energy used by the model [51].

This study aims to provide a new framework for an intelligent data-driven transportation system in metropolitan settings that can display CV data in real-time utilizing a big data analytic engine. It suggests a revolutionary visualization Representational State Transfer (REST) web service, an efficient real-time data distribution strategy, and innovative ways for collecting, extracting, and ingesting data. Through using OMNET++ and Veins, we recreated a traffic incident dataset and put Basic Safety Messages through their paces in a large data cluster experiment. Accurate performance was shown for packet loss, packet delivery, and communication delay; high throughput and low latency were identified for distributed data delivery systems; and the RESTFUL visualization web service exhibited the quickest response time [52].

A novel algorithmic method is hereby provided to organize the cluster structure, and choose CHs suitable for use in a VANET. By improving network settings, Weighted Cluster Protocol (AWCP) achieves the optimal channel by randomly pairing nodes. An automobile network with optimized throughput and location is presented based on a study of the AWCP EE-WOA model. The key generated by each car should be updated regularly, and if a vehicle develops the best method for recognizing keys, the system administrator should suspend or revoke the authority of scenarios. A maximum cluster efficiency of 96.84 is achieved by employing the proposed algorithm, making it superior to both the Weighted Cluster Protocol and the AWCP Whale algorithmic programme protocols in terms of increased encapsulation potency and portability [53].

3. Methodology

This research introduced an improved lightweight authentication scheme for vehicles using a third-party Certification Authority (CA). The CA also monitors traffic in vehicular AdHoc networks (VANETs). We proposed separate registration, authentication, V2V, and V2X communication schemes. We also considered resource allocation and sharing for vehicular communication. To minimize the network signalling overhead of high-speed vehicles, we compared the V2I capacity and vehicle speed. We proposed greedy resource allocation and graph-based baseline resource allocation algorithms. We have implemented our algorithms in MATLAB. For V2V and V2I communication channel establishment, we have developed REST APIs using PHP 8 and MySQL. We analyzed the performance of APIs using a collaborative API development tool called Postman. Our results describe the outclass performance in V2V and V2X communication regarding average End-to-End (E2E) delay, link failure, and secure communication. The maximum returns of our scheme include throughput enhancement, PDR maximization, and TCP connection timeouts. The notions and assumptions are presented in Table 3.

Table 3. Notation Guide.

Notation	Description
V_i	a Vehicle
S	Certification Authority Server
ID_i	Vehicle ID
RN_i	Vehicle Registration Number
$filter\_var()$	Extract Numeric Values from a String
NC_i	Vehicle Numeric Code extracted from the Registration Number
E_i	Vehicle e-mail
PW_i	Vehicle Password
$\|\|$	Concatenation
$h(.)$	One-Way Hash Function
t_i	Vehicle Timestamp
t_s	Server-Side Timestamp
r_i	LCG-Based Random Numbers
VC_s	Vehicle Code generated by the server
SVC_s	Shuffled Vehicle Code using the FYS algorithm
RES_s	The Result computed on the Server-Side
SPW_i	Secured Password for Vehicle
UC_i	Updated Vehicle Code

UC_s	Updated Vehicle Code generated by the server
REF_i	Vehicle Reference
$SUCV_s$	Shuffling of Updated Vehicle Code generated by the server
VCA_s	Vehicle Code for Authentication generated by the server
$SELECT\_RANDOM_s$	OTP-Like Vehicle Code generated by the server
SK_i	Vehicle Session Key generated by the server
AT_i	Vehicle Authentication Method
AS_i	Vehicle Authentication Status
$Message$	Server Response Against HTTP Request
$<>$	Not Equal Operator
lat	Latitude
$long$	Longitude
CL_i	Current Location of the vehicle moving on the road
LUI_i	Vehicle Threshold Location Interval
IT_s	Server Interval Table
LT_s	Server Log Table
$getLatitude()$	The function that will extract latitude from the location
$getLongitude()$	The function that will extract longitude from the location
MP_i	Message Priority
MT_i	Message Template
ID_{rcv}	Receiver ID
ID_{snd}	Sender ID

3.1. Explanation of Notations

- The range of i in V_i varies from 1 to n-1, i.e., $i{:}\{1,2,3.....,n-1\}fti \rightarrow N$, but in other notations, it varies from 0 to $n-1$ i.e., $i{:}\{0,2,3.....,n-1\} \rightarrow W$
- MD5-based secure hash function 128-bit hash value ranges from $h(.){:}\{0,1\}^* \times G \rightarrow Z_q^*$
- r_i such that $i{:}\{0,1,2,3.....,n-1\} \rightarrow W$is presents a set of random numbers generated using the LCG algorithm
- Linear congruential generators can be defined through recurrence relation as:

$$X_{i+1} = (aX_i + c)\, mod\, m$$

- $SELECT\_RANDOM_s$ will generate a 6-digit code.
- SVC_s is generated using the Fisher-Yates shuffle algorithm. Here is the pseudo representation of this algorithm:

```
$for\ i\ from\ n-1\ down\ to\ 1\ do$
$j \leftarrow random\ integer\ such\ that\ 0 \leq j \leq i$
$exchange\ a[j]\ and\ a[i]$
```

- $getLatitude()$ and $getLongitude()$ are two extractor functions that extract latitude and longitude from the input location.
- MT_i contains message templates. These messages might contain the following commands:
    - Please give me the way. I am on your back!
    - Speed up!

- Danger ahead!
- Traffic is jammed on the road. Please adopt an alternative way.
- I run short of fuel. Please help!
- I need a mechanic.
- Tire is punctured.
- There is an accident on the road near my location.
- There is a crowd protesting on the way.
- Please give way to the ambulance!
- Stop on the way. There is a check post.
- The weather condition is bad.

- MP_i contains three values, including 0, 1, and 2. (0) means the priority of this message is nothing. It might be an informative message. 1 means normal priority, while 2 means a very high priority.

4. Proposed Scheme

In this section, we have shown the step-by-step process of our scheme, which we have employed in the authentication and communication schemes for urban traffic monitoring in VANETs based on cluster management.

4.1. Registration Phase

The API needs three parameters in the registration phase of our proposed scheme:

- e-mail
- Password
- Vehicle Registration Number

The API will get the current time on the vehicle onboard unit side. The other operations include encrypting passwords using MD5, extracting numeric values from vehicle registration numbers, generating updated codes, and creating reference values for vehicles OBU. The $filter\_var()$ function takes the registration number as input, and returns all numeric characters from the input string in our scenario. After extracting the NC_i, this NC_i is concatenated with ID_i API from the database which fetches that. For example, if there is no registered vehicle on the CA Server, the database will return 0, and API will increment the value by 1 in ID_i. We have applied the SQL aggregate MAX function that will return the maximum ID_i stored in the table. The combined value of ID_i and NC_i is assigned to UC_i. A lightweight block is created to prevent database record tempering in the form of a field that takes ID_i, t_i, and r_i as inputs, and merges these values using the concatenation operator, and produces the vehicle registration reference REF_i. The API sends $\{ID_i, E_i, SPW_i, UC_i, REF_i\}$ on a public channel. The Certification Authority Server generates Updated Vehicle Code UC_s by taking UC_i and a random number r_2. The $UC_s$is shuffled using the function $shuffle()$ to form SVC_s. This SVC_s is then passed to $SELECT\_RANDOM()$ function in order to produce VCA_s. This VCA_s can be used for authentication henceforth. After all this processing, the Certification Authority Server stores $\{ID_i, E_i, SPW_i, UC_i, UC_s, SV_s, VCA_s, REF_i\}$ in the DB table. The CA Server also generates Session Keys for the onboard vehicle unit. The SK_i is generated by combining ID_i and t_s. The CA Server sends $\{SK_i, VCA_s\}$ to the OBU after handling all the processes mentioned above. Finally, the OBU stores $\{SK_i, VCA_s\}$ in its shared preferences for session management.

OBU	CA Server
Registration:	
Selects ID_i|, E_i, PW_i and RN_i	
Computes	

t_i		
$SPW_i = h(PW_i)$		
$NC_i = filter\_var(\, RN_i)$		
$UC_i = (ID_i\|\|NC_i)$		
$REF_i = (ID_i\|\|t_i\|\|r_1)$		
	$\xrightarrow{\{ID_i,E_i,SPW_i,UC_i,REF_i\}}$	$UC_s = (UC_i\|\|r_2)$
		$SVC_s = shuffle(UC_s)$
		$VCA_s = SELECT\_RANDOM(SVC_s)$
		Store
		$\{ID_i, E_i, SPW_i, UC_i, UC_s, SV_s, VCA_s, REF_i\}$
		Generates
Insert $\{SK_i, VCA_s\}$ inside vehicle OBU		$SK_i = (ID_i\|\|t_s)$
	$\xleftarrow{\{SK_i,VCA_s\}}$	

4.2. Authentication Phase

In the authentication phase, there are two possibilities for authentication with the Certification Authority Server. Authentication can be done using e-mail or password, or the authentication code obtained in the registration phase. After selecting any login method, t_i is computed by the OBU for updating the logs table. AT_i is passed to the server along with its corresponding parameters. The CA Server checks the authentication type. We set two threshold values, i.e., 0 for VCA_s and 1 for E_i, PW_i. If AT_i == 0, then the CA Server compares VCA_s with database records. If the vehicle code already exists in the database, the server sends a response with a success message and starts the OBU session. The CA Server also updates the logs table for log maintenance. Otherwise, the server sends a failure message in response and does not start the OBU session on failure. It is clear from threshold values that 0 is for VCA_s, and 1 is for E_i, PW_i that is why when the CA Server receives AT_i== 0, the server compares E_i, PW_i with database records. If records match, the server sends a response with a success message, starts the OBU session, and updates the log table. Otherwise, the CA Server sends a failure message in the response and does not start the OBU session. The server sends $\{SK_i, Message\ \}$ as a response to the OBU. The OBU checks the response; if $Message ==$ "$Success$" and $SK_i <> null$then OBU sets $AS_i =$ "OK"; otherwise $AS_i =$ "$Failed$".

Vehicle OBU	CA Server
Login and authentication:	
Inputs E_i, PW_i OR VCA_s	
Computes	
t_i	
ID_i	
REF_i	
AT_i	

	$\xrightarrow{ID_i, REF_i, ((E_i, PW_i) OR (VCA_s)), AT_i\}}$	Checks AT_i $if(AT_i == 0)$ Compares VCA_s with DB $if(mathched)$ $Message = “Success”$ $SK_i = (ID_i \| \| t_s)$ Updates logs table $else$ $Message = “Re t ry”$ $SK_i = null$ $else$ compares E_i and PW_i with DB $if(mathched)$ $Message = “Success”$ $SK_i = (ID_i \| \| t_s)$ Updates logs table $else$ $Message = “Re t ry”$ $SK_i = null$
$if((Message == “Success”)\&\&$ $(SK_i <> null))$ $AS_i = “OK”$ $else$ $AS_i = “Failed”$	$\xleftarrow{SK_i, Message}$	

4.3. V2I Communication

V2I communication is only possible when the vehicle is registered on the CA Server and has an active session. On the vehicle side, The OBU computes ID_i, REF_i, CL_i, LUI_i, and t_i. CL_i is composed of the latitude and longitude of the vehicle. The CA Server gets $\{ID_i, REF_i, CL_i, LUI_i, t_i\}$ as parameters. ID_i, REF_i, t_i and, t_s are concatenated to form IT_s. If the CA Server receives a value regarding the current location of the OBU, it extracts latitude and longitudes from CL_i. Otherwise, it returns null values in response. The parameters $\{lat, long\}$ are then passed to the vehicle for parsing purposes.

Vehicle	**CA Server**
V2I Communication: Computes ID_i REF_i $CL_i = (lat + long)$	

LUI_i t_i		
	$\xrightarrow{\{ID_i,REF_i,CL_i,LUI_i,t_i\}}$	$IT_s = (ID_i \Vert REF_i \Vert t_i \Vert t_s)$ Updating logs $LT_s = (ID_i \Vert REF_i \Vert CL_i, LUI_i, t_i)$ $if(CL_i <> null)$ $lat = CL_i.getLatitude()$ $long = CL_i.getLongitude()$ $else$ $lat = null$ $long = null$
Parsing $\{lat, long\}$	$\xleftarrow{\{lat,long\}}$	

4.4. V2V Communication

In V2V communication, Vehicle A selects ID_{rcv}, MTi and MP_i. The $Message$ is composed of MTi and MP_i. Vehicle A, through APIs, sends $\{ID_{snd}, ID_{rcv}, message, t_i\}$ as parameters to Vehicle B. After the $message$ acknowledgement, Vehicle B can reply to Vehicle A, but doing so is optional.

Vehicle A		Vehicle B
V2V Communication: Selects ID_{rcv}, MTi and MP_i Computes $Message = (MTi + MP_i)$ ID_{snd} t_i		
	$\xrightarrow{\{ID_{snd},ID_{rcv},message,t_i\}}$	Acknowledgement of $message$ Replies: ID_{snd} $=ID_{rcv}$ Selects MTi and MP_i Computes $Message = MTi$ ID_i t_i
Acknowledgement of $message$	$\xleftarrow{\{ID_i,message,t_i\}}$	

4.5. Vehicle Clustering and Monitoring

One Certification Authority (CA) in a VANET authenticates all the vehicles within a 400-meter cluster. The cluster may include 100-meter range sub-clusters as per the topology of the VANET. The CA is a trusted third-party that manages registration, authentication, and vehicle communication record registers. The vehicles moving on the highway are divided into several clusters. Each cluster has one Cluster Head (CH) and one or more cluster members. The cluster has two bands, each with one or more lanes. All the vehicles inside the cluster are inter-connected directly and can communicate with each other. Outside the cluster, communication vehicles can communicate using corresponding Cluster Heads. Figure 3 shows the lattice of our proposed VANET for V2V and V2I communications. The range of clusters in this scenario is 400 meters. The main cluster is subdivided into a 100-meter range for each. The CA performs the registration, authentication, monitoring, and allowing vehicles' communications. The base station provides the network link to CH and CA.

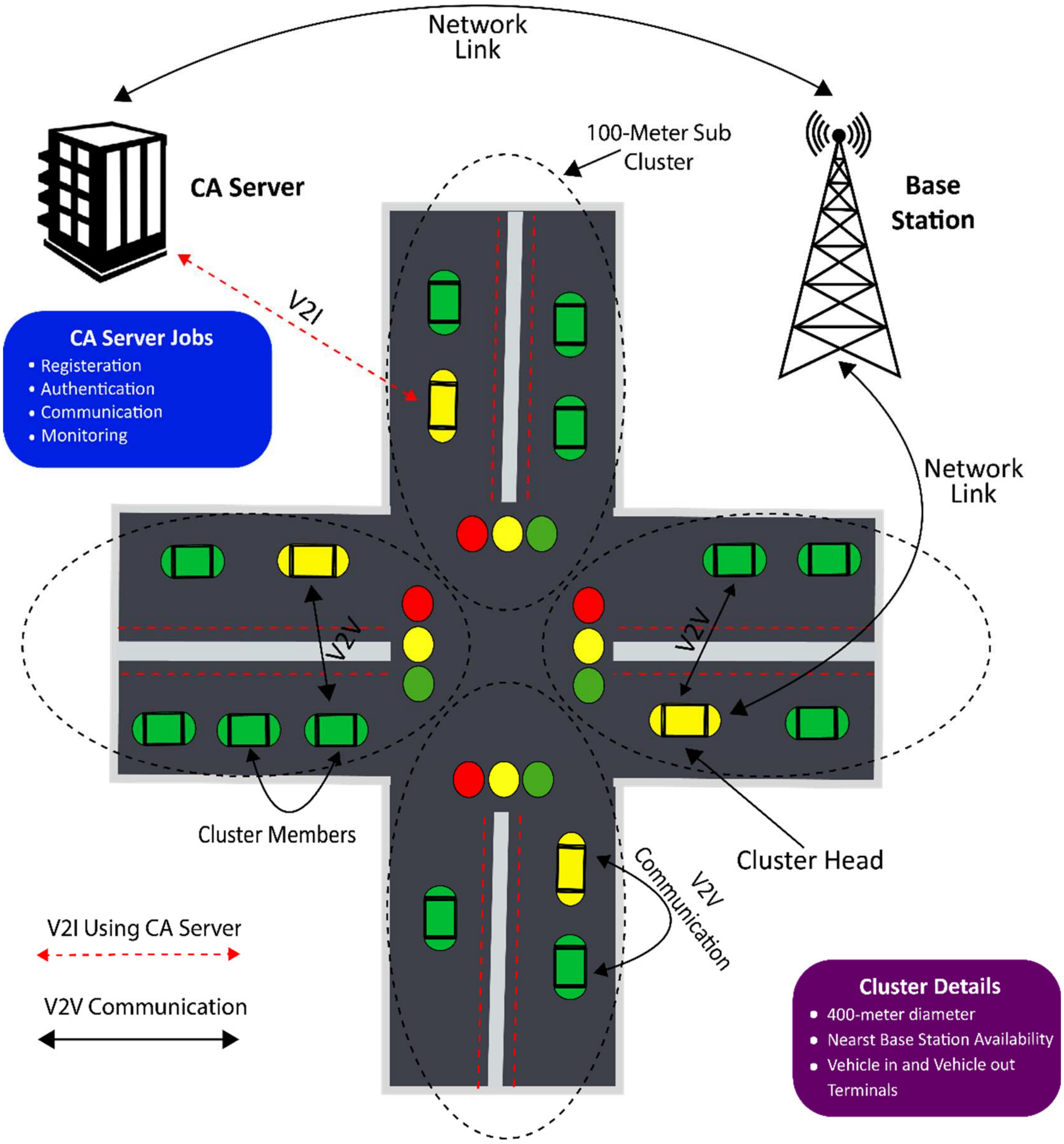

Figure 3. V2V and V2I Communication on our proposed VANET.

Selecting the Cluster Head is described in Algorithm 1, while the topology of traffic flow in different types of clusters in VANET is described in Figure 4. In the monitoring phase, the CA collects the behavioural information of all vehicles in a cluster. For example, the reported vehicle's information, the maintenance vehicle's communication register, and the number of vehicles in a specific interval cluster. The authentication phase of our proposed scheme addresses this issue.

4.6. Cluster Head Selection Algorithm

1. Each vehicle inside a cluster announces itself as a "Cluster Head" and displays the broadcast signal: $S[Id_i, POSITION_i]$.
2. Every vehicle V_j displays the list of closest vehicles (VL_i) after getting $S[Id_i, POSITION_i]$ from V_i.
3. $DISTANCE_{ij}$ is estimated by V_j.
4. Weighted sum is calculated by V_j:

   $W_j = a\,NV_j + bR + c\theta_i + dS_i$
   The vehicle calculates the above equation's arguments, and the range of weighted constants varies from 0 to 1. Since the weighted sum is derived from these arguments, the Cluster Head based on this sum will be the most efficient and trustworthy.

5. In the end, the V_i with the lowest W_j is selected as the Cluster Head.

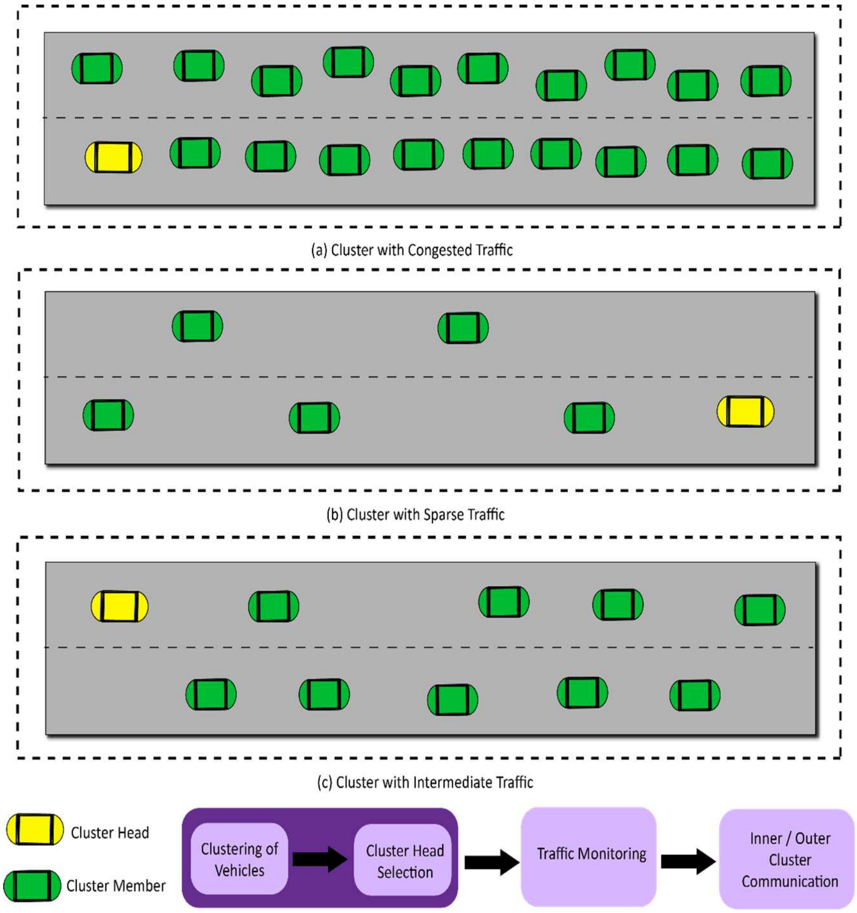
(a) Cluster with Congested Traffic
(b) Cluster with Sparse Traffic
(c) Cluster with Intermediate Traffic
Cluster Head
Cluster Member
Clustering of Vehicles
Cluster Head Selection
Traffic Monitoring
Inner / Outer Cluster Communication

Figure 4. V2V and V2I Communication in a cluster.

Notations	
V_i	a Vehicle
ID_i	Vehicle Unique Identity
V_j	Closest Vehicle
$POSITION_i$	Vehicle-ID
VL_i	Closest Vehicles List
$DISTANCE_{ij}$	Distance Between V_i and V_j
NV_j	Number of Closest Vehicles to V_j
R	Range of Dynamic Transmission
θ_i	Moving Vehicle Direction
S_i	Vehicle Speed
a, b, c, d	Assumed Weights

5. Simulation Setup and Experiments

For experimental purposes, we formed three clusters featuring (a) congested traffic, (b) sparse traffic and (c) intermediate traffic, as shown in Figure 4. Each cluster band has two lanes, and each lane has at least one or more vehicles obeying the instructions of the CH vehicle; which is a unique vehicle in a cluster. We wrote our web services as restful APIs in PHP to implement our proposed scheme. We employed the most recent PHP (PHP 8) version and MySQL to maintain CA vehicle communication and monitoring registers. We send five different HTTP requests using the HTTP GET method. We applied the Postman tool for API performance evaluation, and noted the results obtained from several scenarios. We also worked on the resource allocation of V2V and V2I communication with the help of two algorithms and MATLAB simulation. To measure the security and message delivery, we compared our simulation results with the research work of Sugumar et al. [59]. In this regard [59], the authors proposed authentication techniques for cluster-based VANET. The authors simulated their proposed scheme using an open-source Network Simulator Version 2 known as NS2. NS2 is frequently used by researchers in computer communications and networking-related research, especially wireless networks. The authors further compared their research with the works of other researchers and displayed the efficiency of their proposed technique. Our main focus is to compare their technique with ours. First, we compared our scheme's resultant authentication delay, detection accuracy, keying overhead, and packet delivery ratio [59]. Later, we compared the transmission range in the context of packet delivery, authentication delay, keying overhead, and detection accuracy.

5.1. Varying the Attackers

To inspectf our proposed scheme's authentication delay, we set the transmission range to 400. We counted the average authentication delay of clusters having been congested, average, and sparse traffic, respectively. Each cluster's number of attackers or malicious vehicles varied from 1 to 5. Figure 5 depicts the average authentication delay in milliseconds for all DDoS attacks and mitigation methods, including HTTP Flood, Ping of Death, NTP Verification, and Slowloris. The results indicated a better performance compared to the experiment carried out by Sugumar et al. [59].

Moreover, the authors of [59] did not test their scheme on different types of clusters. It compares our Improved Authentication and Communication Scheme (IACS) results with the experimental results of the authors [59]. For comparison, we did not show the different authentication delays for each congested, average, or sparse cluster. We calculated each cluster's average authentication delay, and compared it with the number of attackers. Our scheme also provided efficient results regarding Detection Accuracy and Keying Overhead. Figure 6 demonstrates Detection Accuracy; when the number of attackers increased, the detection accuracy decreased in all three schemes. Figure 7 shows the Keying Overhead of our scheme concerning the scheme of [59]. Since the experiment of Sugumar et al. [59] includes a complex keying generation process, their results do not provide better results than ours. In Figure 8, we compared the packet delivery ratio in the context of varying attackers with the results of Sugumar et al. [59]. Our results indicate a better performance compared to that obtained by the authors [59].

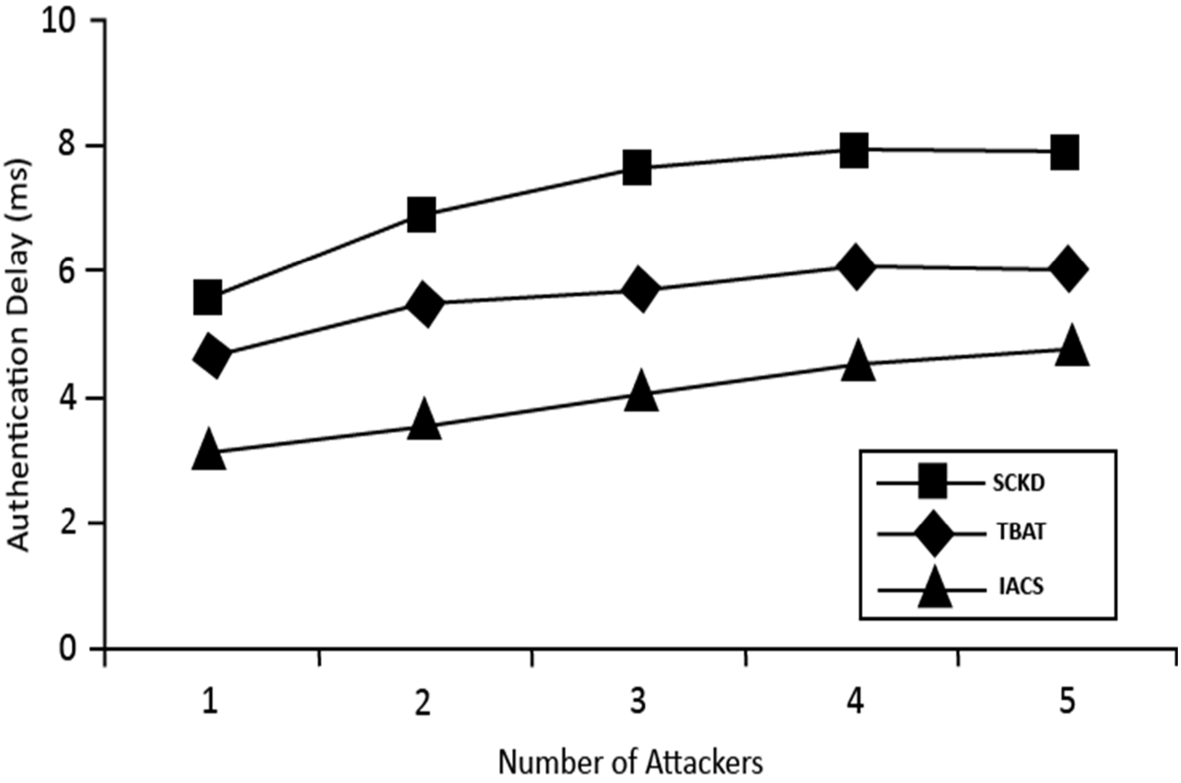

Figure 5. Authentication Delay vs. Number of Attackers.

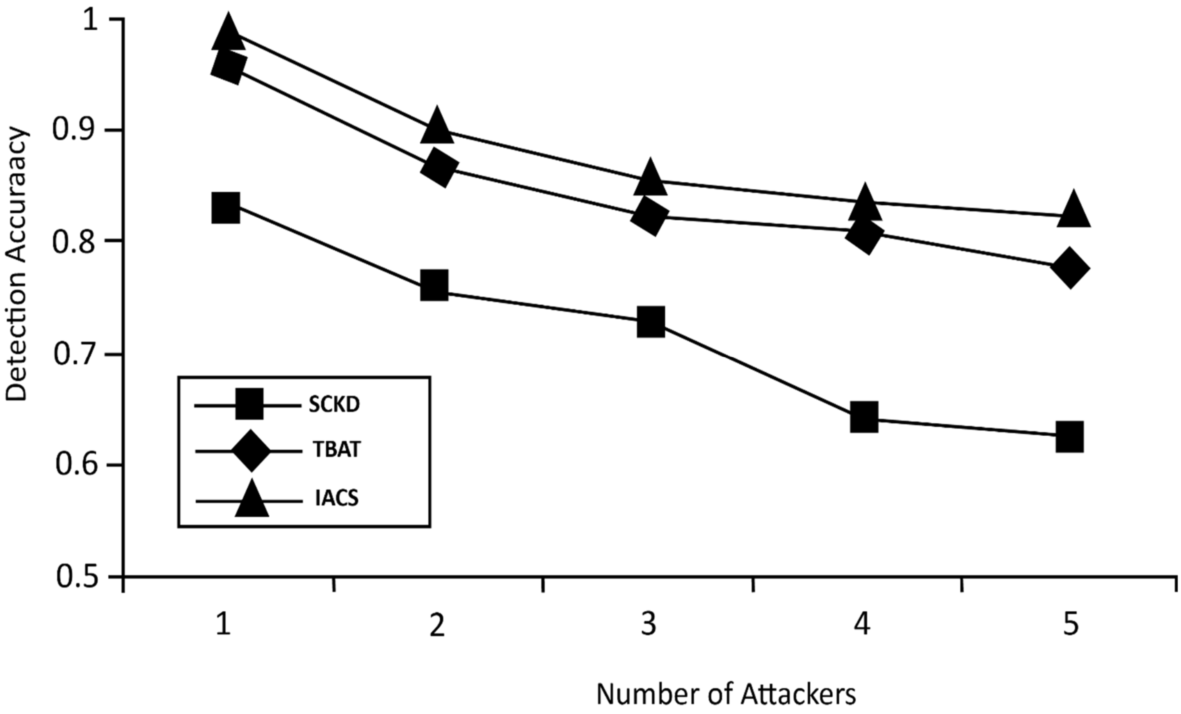

Figure 6. Detection Accuracy vs. Number of Attackers.

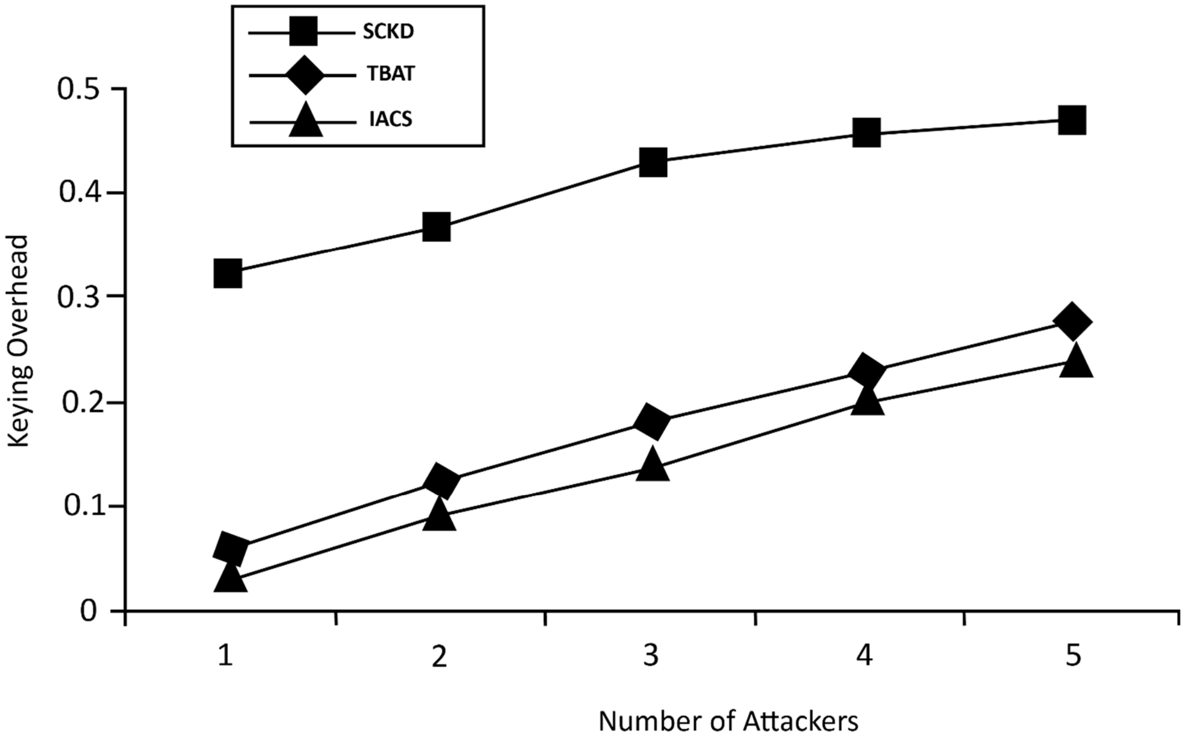

Figure 7. Keying Overhead vs. Number of Attackers.

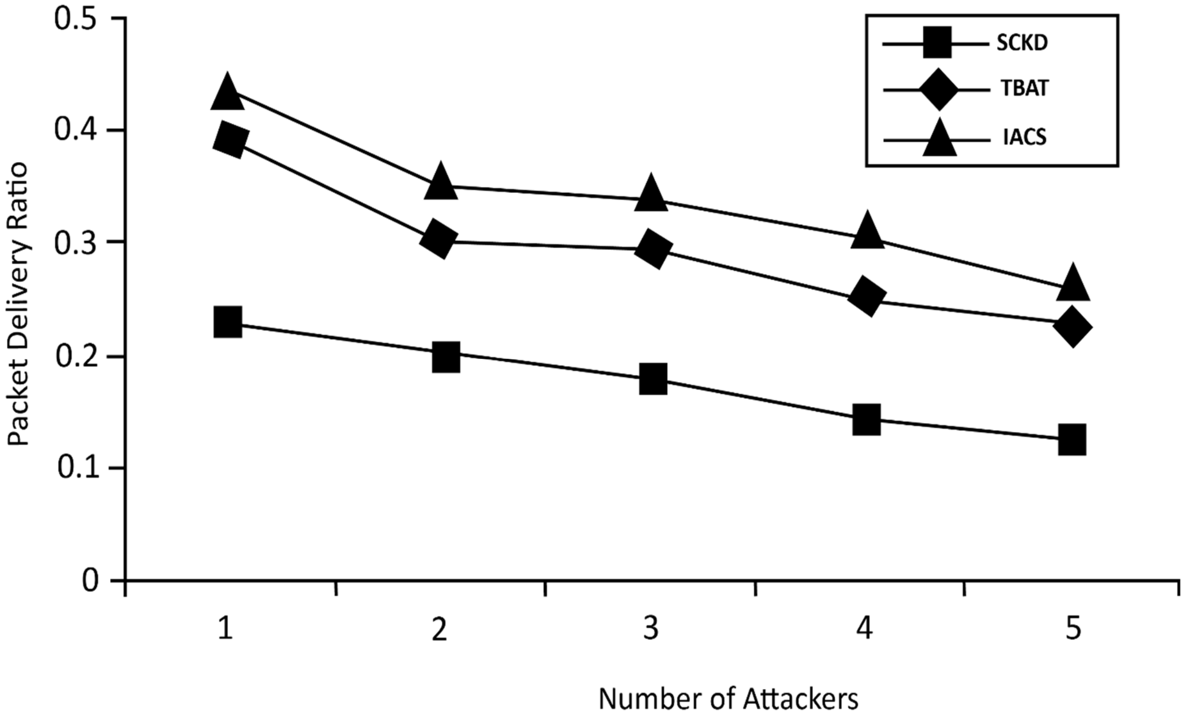

Figure 8. Packet Delivery Ratio vs. Number of Attackers.

5.2. Transmission Range

In our next experiment, we noted the sub-cluster effect on the transmission range. We formed a 400-meter cluster with varying speeds. Through this method, we noted the average packet delivery ratio of three clusters (Congested, Sparse, and Intermediate) concerning the corresponding cluster range. For the Postman simulation, we supposed that the location of the base station is fixed at a certain point. The routing delay will occur as the vehicle moves in a corresponding cluster. We also supposed that the delay factor in routing would increase when the range is increased. Figure 9 shows a comparison of Cluster Range and Packet Delivery. Our proposed Improved Authentication and Communication Scheme (IACS) results perform much better than those obtained by Sugumar et al. [59], as shown in Figure 9. In Figure 10, we have compared Authentication Delay, while Figure 11 shows Keying Overhead in the context of varying cluster ranges. In Figure 12, we have compared the Detection Accuracy with the results obtained by [59]. It is observable that our scheme has also provided a much better performance in varying cluster ranges.

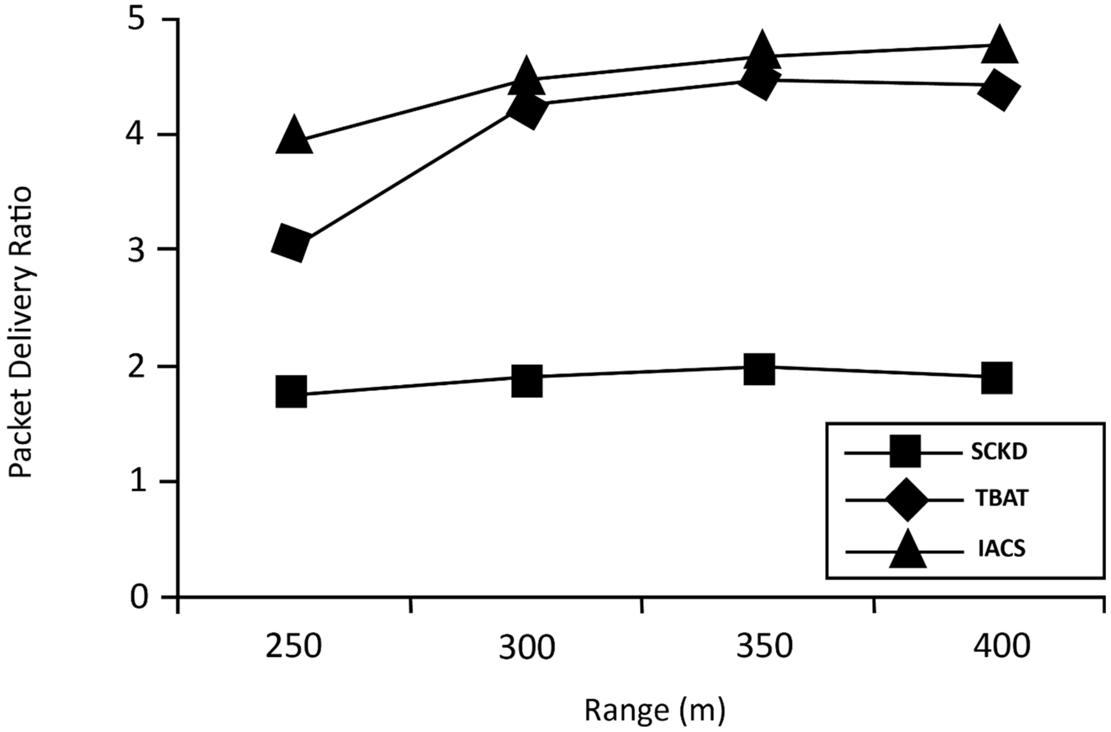

Figure 9. Delivery Ratio and Cluster Range Comparison.

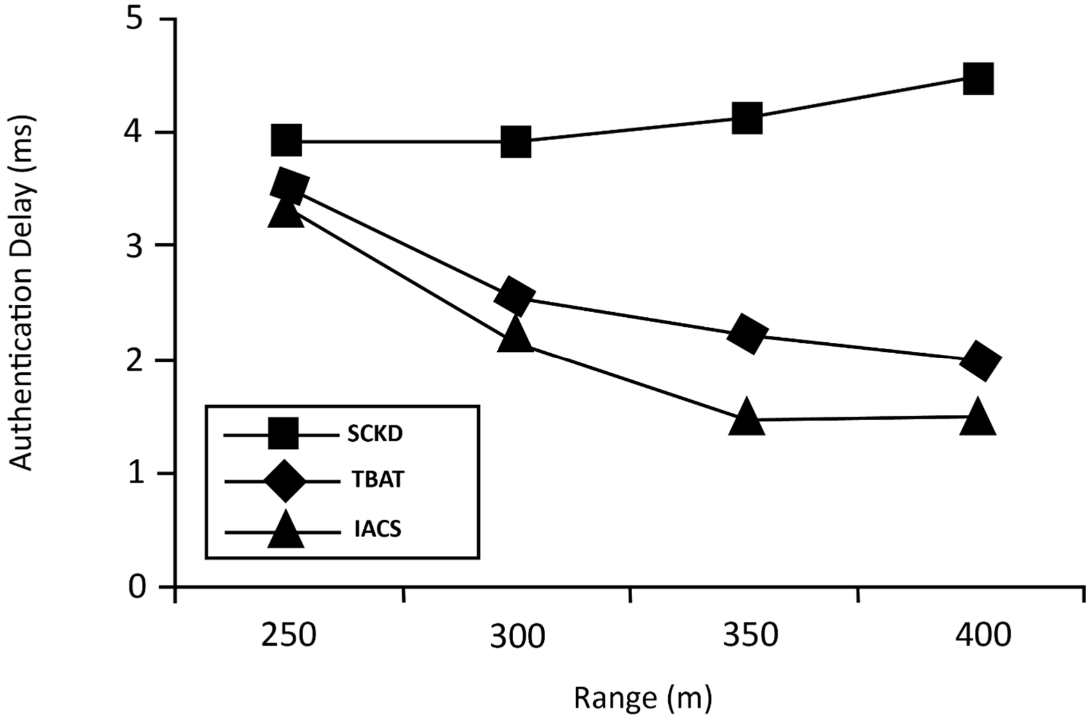

Figure 10. Authentication Delay and Cluster Range Comparison.

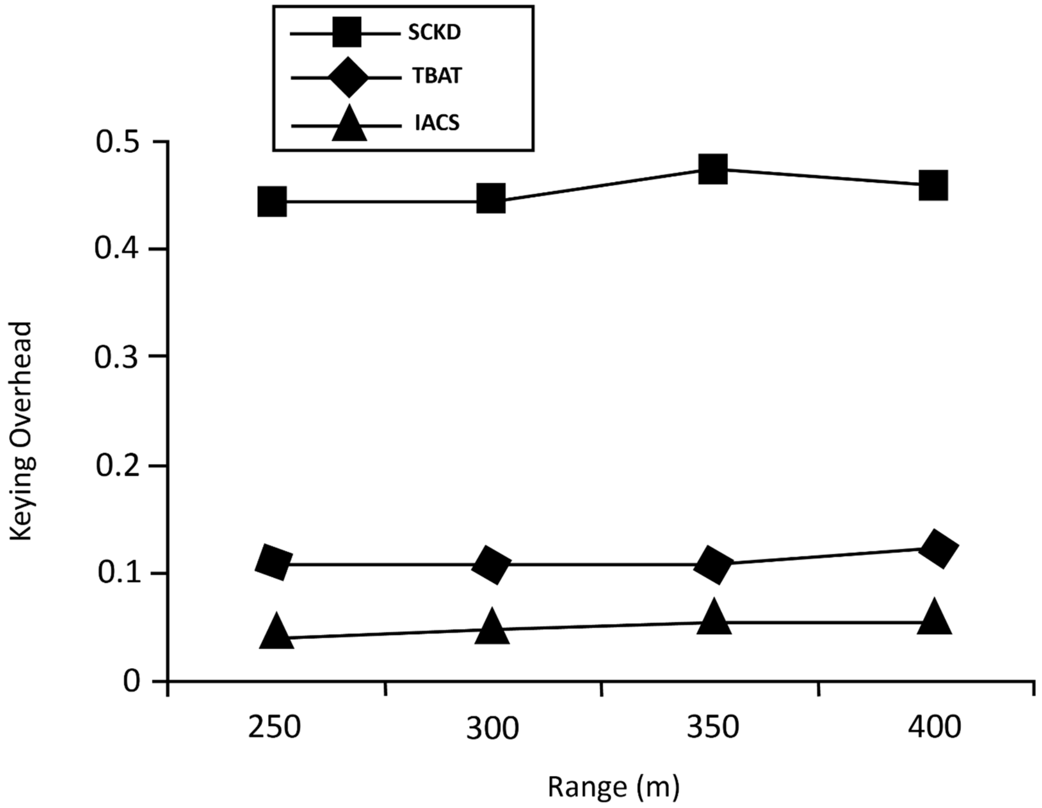

Figure 11. Keying Overhead and Cluster Range Comparison.

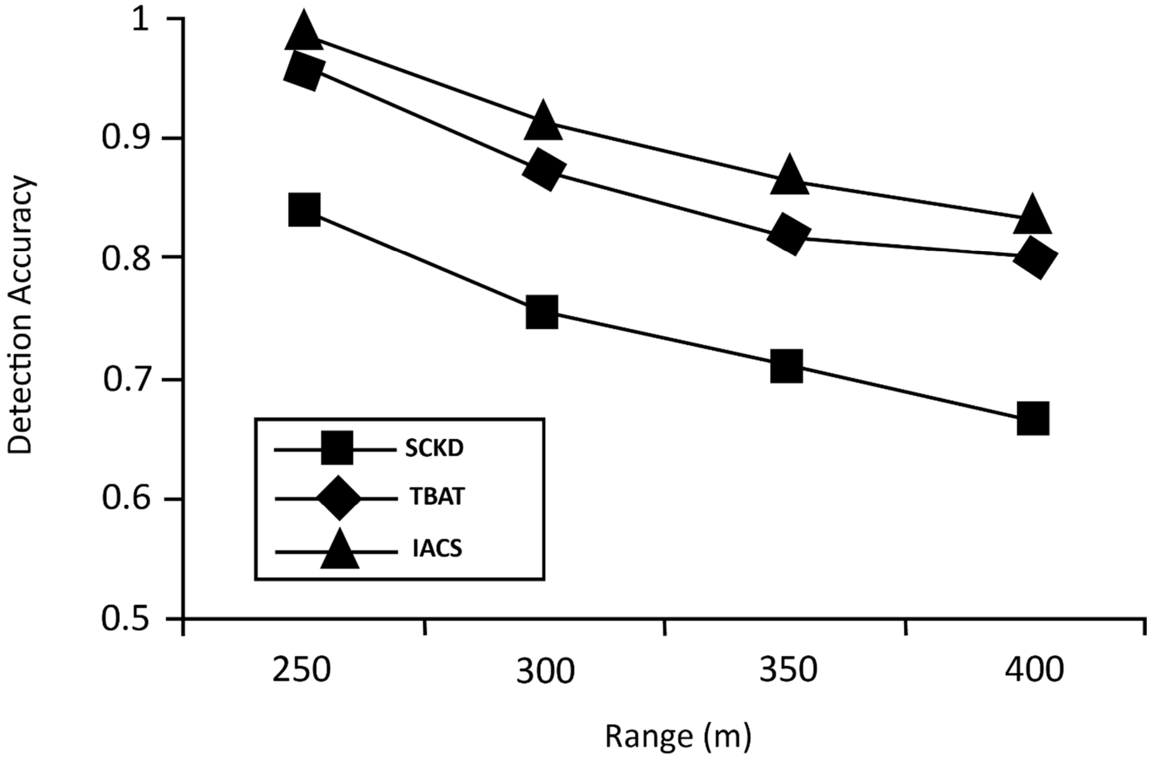

Figure 12. Detection Accuracy and Cluster Range Comparison.

5.3. Baseline Graph-Based Resource Allocation

The optimization of resources in high-mobile vehicles is a significant issue. We introduced a baseline low-complexity algorithm. To achieve this milestone, we first assigned an arbitrary V2V link to all clusters specified in Figure 3, and then simulated our baseline graph-based resource allocation approach using MATLAB. Table 4 presents the algorithm of our proposed resource optimization and allocation method.

Table 4. Baseline Graph-Based Resource Allocation.

Baseline Graph-Based Resource Allocation Algorithm

```
Arbitrarily allocate one V2V link to every cluster from C clusters ($C_1$, …… $C_n$).
for m = 1: M do
    for n = 1: N do
        for f = 1: F do
            Compute the V2I optimal transmit power using the algorithms provided by [64].
            Compute the V2V optimal transmit power using the algorithms provided by [64].
            Compute the V2I and V2V power gain capacity from the base station resource blocks with the
            optimized power control parameters.
        end for
    end for
end for
Construct a tripartite graph; where M shows V2I links, while N is a V2V link.
Return the power allocation using resource blocks.
```

Figure 13 shows the Cumulative distribution function (CDF) of the quick Signal-to-Interference-Plus-Noise Ratio (SINR) of V2V and V2I communications using our proposed graph-based resource allocation algorithm.

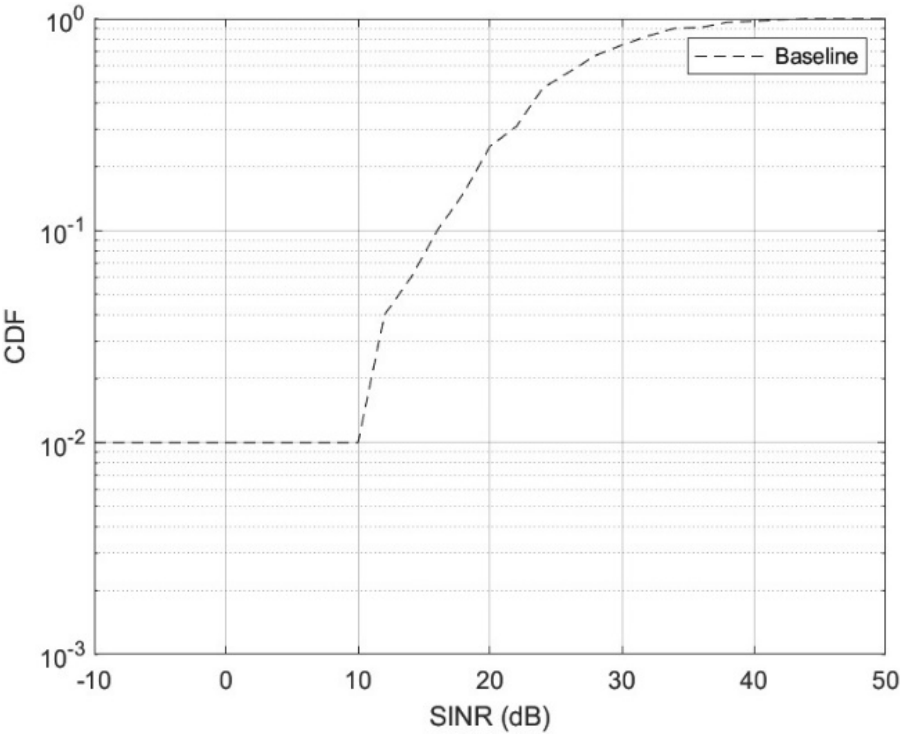

Figure 13. Cumulative Distribution Function (CDF) of Instantaneous Signal-to-Interference-Plus-Noise Ratio (SINR) of V2V and V2I Communications.

In Figure 14, we have merely discussed the Sum of V2I capacity with varying vehicle speeds by adopting the algorithm provided by [64] in our algorithm. V2V transmit power in dBm is taken as 33. Large-scale fading parameters are V2V = 3 and V2I = 8, which are shadowing standered deviation. Cell parameter setup is done in such a way that the carrier frequency is 3.5 GHz, 200 cell radius in meters, base station height 25 meters, 35 meters BS-highway distance in meters, and base station noise is 5dB. The vehicle antenna height is 1.5 meters, with the vehicle antenna gain of 3 dBi and the vehicle noise being 9 dB. The number of lanes is reduced from 6 to 4, and the lane width is reduced from 4 to 3 meters. The velocity range is from 20 to 160. According to TR 36.885, the average inter-vehicle distance is 2.5*v/3.6. The maximum number of links for V2I is reduced from 10 to 5 [32].

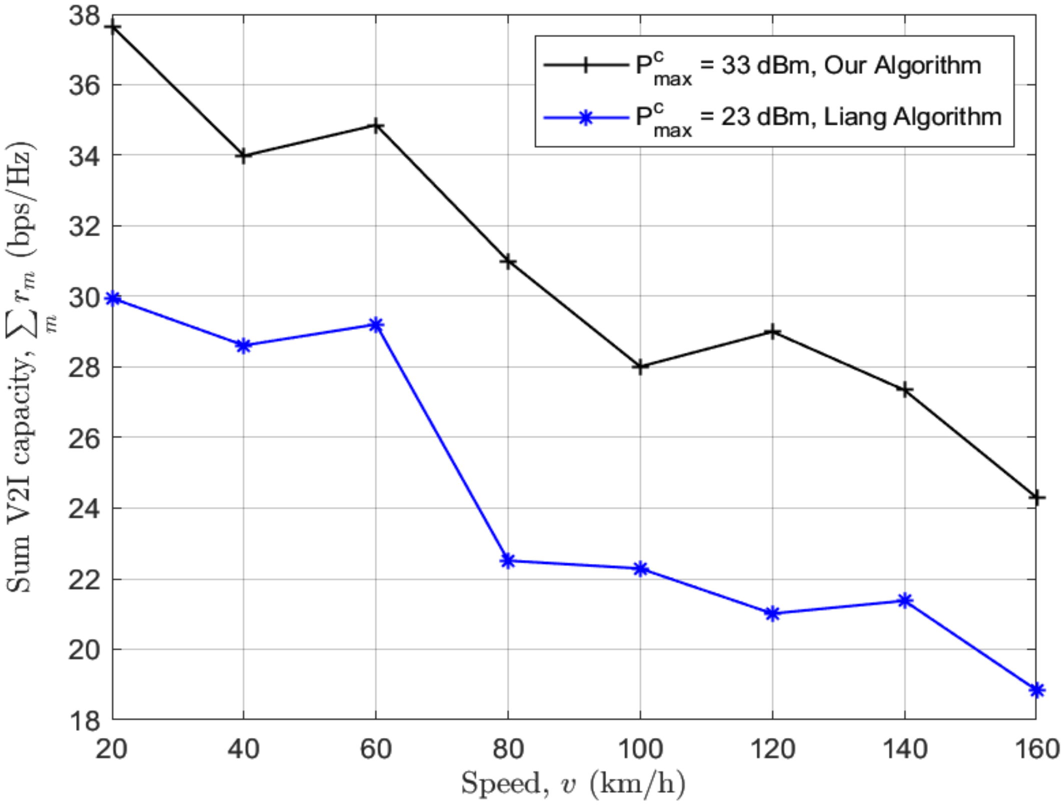

Figure 14. Sum of V2I Capacity with Varying Vehicle Speeds.

5.4. Greedy Resource Allocation

We proposed an additional algorithm based on the Greedy Approach grounded on the baseline graph-based resource allocation algorithm. Table 5 shows the algorithm of our proposed greedy approach.

Table 5. Greedy Resource Allocation.

Greedy Resource Allocation Algorithm	
1.	Obtain V2V and V2I clustering results from baseline graph-based resource allocation algorithm.
2.	Repeat the process.
1.	for k = 1: K do
2.	Initialize all zero vectors having a length of N.
3.	for n = 1: N do
4.	If kth V2V is not only in its current cluster C,
5.	then set C_k = n

```
            end if
        end for
    end for
Return the power allocation using resource blocks.
```

Figures 15 and 16 show the simulation results of the baseline greedy resource allocation algorithm:

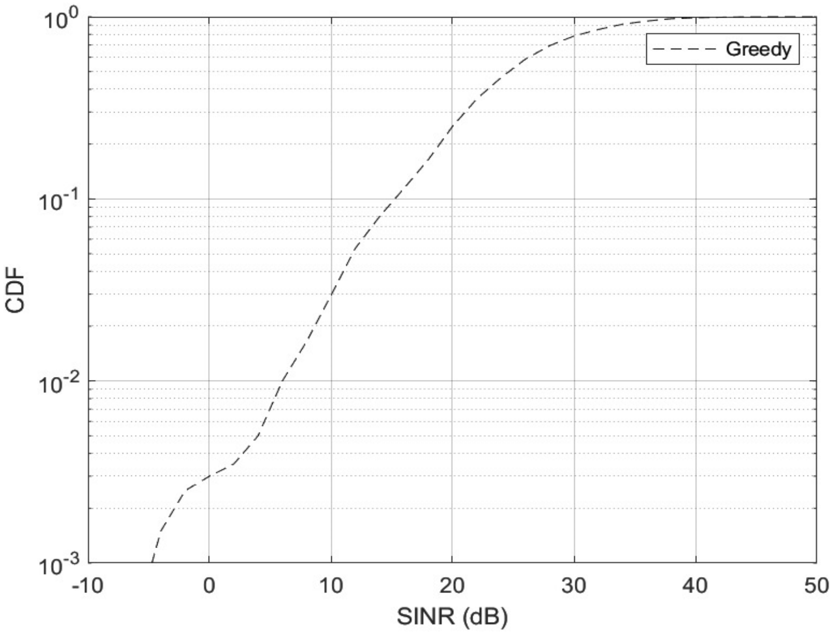

Figure 15. Cumulative Distribution Function (CDF) of Instantaneous Signal-to-Interference-Plus-Noise Ratio (SINR).

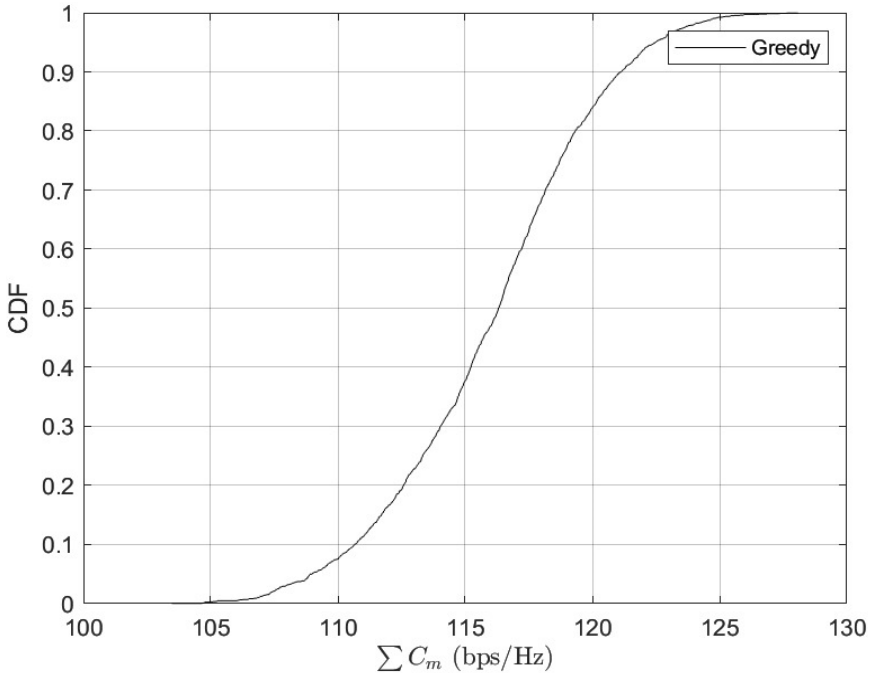

Figure 16. Cumulative Distribution Function (CDF) Concerning the Sum of V2I Capacity.

5.5. V2I and V2V Communications

In order to generate our results, we employed Postman and noted the response time breakdown provided by the tool. We focused on considering significant factors, such as API status and API response size, socket initialization, DNS lookup, TCP handshake, Transfer rate, and download rate. We discarded some factors, for instance preparation time and response headers, owing to the fact that they are minor factors. Results can be shown through a single HTTP request, but we tested our developed API against 5 different HTTP requests for better evaluation. Table 6 shows the API response time of 5 different requests. Here, the status code of the API hit is 200, meaning the response is in an "OK" state. The response size is the same (289 bytes) for each request, while the response times of other parameters vary from instance to instance. Since our APIs provided successful responses to every HTTP request, the server sends the JSON response to the vehicle (client side) on each request. Vehicular communication on 5G VANET using RESTful APIs is a novel concept and can revamp the overall performance of the VANET. Our algorithms also include security and privacy features; and with the introduction of RESTful APIs, an extra layer of security is added to this client-server model deployed for vehicular communication over the VANET. Due to the high bandwidth and fast communication rate in 5G, the proposed algorithm will provide a robust packet delivery ratio and faster API response, as shown in Table 6.

Table 6. API Response for 5 Random HTTP Requests.

Vehicle-to-Infrastructure (V2I)					
Attributes	1st Request	2nd Request	3rd Request	4th Request	5th Request
Status (status code)	200	200	200	200	200
Response Size (bytes)	289	289	289	289	289
Socket Initialization (milliseconds)	2.18	2.07	1.77	2.12	1.40
DNS Lookup (milliseconds)	4.11	3.19	2.95	2.17	1.62
TCP Handshake (milliseconds)	1.47	1.25	1.06	0.92	0.76
Transfer Start (milliseconds)	91.38	98.18	88.02	82.33	80.91
Download (milliseconds)	20.24	4.19	3.35	4.81	3.73
Vehicle-to-Vehicle (V2V)					
Status (status code)	200	200	200	200	200
Response Size (bytes)	289	289	289	289	289
Socket Initialization (milliseconds)	11.24	4.22	1.68	1.36	1.04
DNS Lookup (milliseconds)	1.19	0.48	0.77	0.47	0.89
TCP Handshake (milliseconds)	3.03	1.48	2.49	2.63	2.41
Transfer Start (milliseconds)	91.75	93.56	83.26	62.03	58.95
Download (milliseconds)	12.61	4.49	2.89	3.32	3.45

5.6. Performance Evaluation of V2V and V2I Communications

Due to the API's streamlined code and small size, the response time data provided a tremendous performance since data on the client side are present in a stateless form, which is why RESTful APIs

doi:10.20944/preprints202305.0683.v1

also allow cache storage. We cleared the Postman cache to measure all attributes' numeric values on each response, but the response time provides a much faster rate after cache storage. Figures 17 and 18 present the overall performance of V2I and V2V communications, respectively.

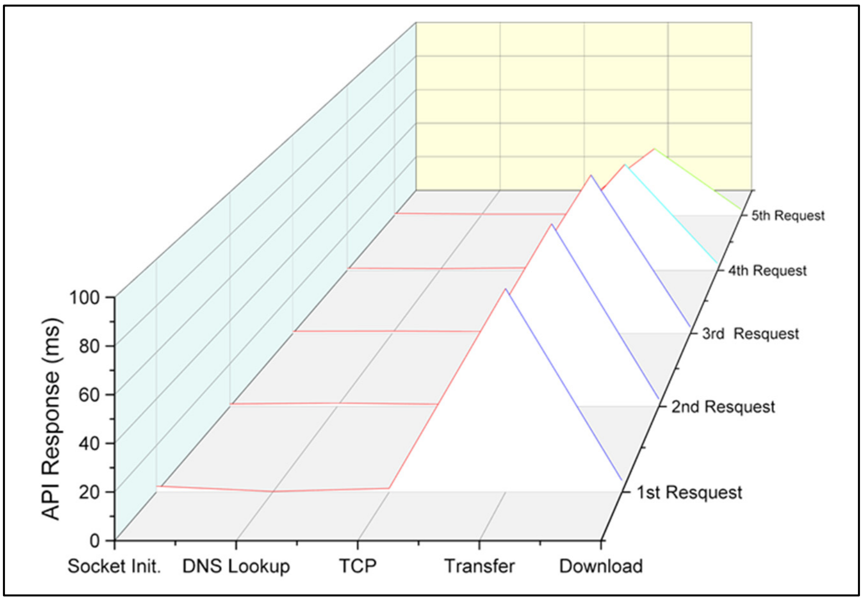

Figure 17. Performance Graph of Vehicle-to-Infrastructure (V2I) Communications.

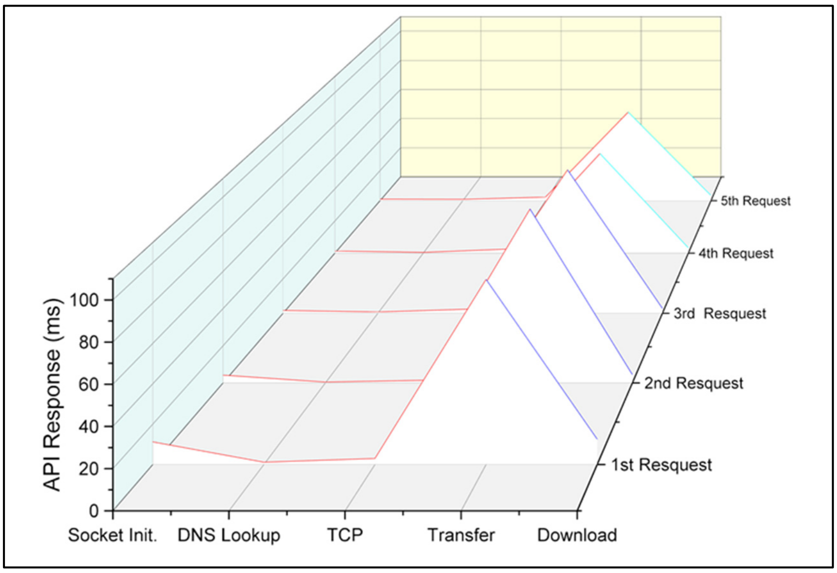

Figure 18. Performance Graph of Vehicle-to-Vehicle (V2V) Communications.

6. Conclusions

This research covered a broad spectrum of vehicular communications on VANET. We proposed the cluster-based improved authentication and communication resource-sharing algorithms for vehicular communications. The use of cluster-based routing schemes for V2V and V2I communication enhances the reliability, scalability, and stability of fast-moving VANETs. The third-party certification authority for vehicle authentication provides a secure and private mechanism for authentication. The schemes minimize the E2E delay and route request, reduce link failure, and improve the throughput, TCP Socket Initialization time, TCP handshake response, and DNS lookup. The innovative P2P wireless communication in a 400-meter radius cluster minimizes the resources used, and the RESTful APIs and algorithms for resource sharing enable implementation in vehicular communication. Our experimental evaluation demonstrates the effectiveness of the proposed schemes in optimizing resource sharing in vehicular communication. The proposed scheme can contribute to the development of more efficient and reliable Intelligent Transportation Systems in VANETs, which can improve the traffic management and reduce congestion in overcrowded city zones. For simulation and performance evaluation, we used MATLAB and REST APIs. Finally, the results of this study were compared with those obtained through relevant past studies, suggesting an improved performance through cluster-based authentication and communication scheme.

Since the 5G network diminishes the internet speed barrier and other issues related to VANETs communication, our proposed improved cluster-based authentication and communication scheme will provide accelerated performance in V2I and V2V communications. It is also helpful in developing real-world apps in the future by adopting this secure and reliable scheme. One future trend in the area of urban traffic monitoring in VANETs (Vehicular Ad-hoc Networks) based on cluster management is the integration of blockchain technology. Blockchain can provide a secure and decentralized way of managing the clusters and nodes in VANETs, enhancing the security and privacy of the communication and authentication schemes. Another trend is the use of artificial intelligence and machine learning algorithms to improve the accuracy and efficiency of the traffic monitoring and management. These techniques can help in identifying patterns, predicting traffic congestion, and optimizing traffic flow. Moreover, the use of IoT (Internet of Things) sensors and devices, such as cameras and traffic sensors, can be integrated into VANETs for collecting real-time data and improving the accuracy of traffic monitoring and management. Finally, the development of new communication protocols and standards for VANETs can also be expected. The focus will be on enhancing the reliability, security, and privacy of the communication schemes, as well as ensuring interoperability and compatibility with other networks and systems.

References

1. Jithendra, H. and D. Rekha, *Secured Trusted Authentication with Trust-Based Congestion Scheme for V2V Communication*, in *Cloud and Fog Computing Platforms for Internet of Things*. 2022, Chapman and Hall/CRC. p. 157-168.
2. !!! INVALID CITATION !!! .
3. Cui, J., et al., *Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme.* IEEE Journal on Selected Areas in Communications, 2020. **38**(6): p. 1191-1204.
4. Hamzah, M., et al., *Distributed Control of Cyber Physical System on Various Domains: A Critical Review.* Systems, 2023. **11**(4): p. 208.
5. Goyal, A.K., et al., *Systematic Study of VANET: Applications, Challenges, Threats, Attacks, Schemes and Issues in Research*. Green Computing in Network Security. 2022. 33-52.
6. Singh, M., C. Kumar, and P. Nath, *P2P Applications in 4G/5G Networks Using D2D Communication Based on Social Attributes of Users.* 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2020: p. 730-738.
7. Hamdi, M.M., et al. *A review of applications, characteristics and challenges in vehicular* ad hoc *networks (VANETs)*. in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. 2020. IEEE.
8. Hsieh, F.-S., *Improving Acceptability of Cost Savings Allocation in Ridesharing Systems Based on Analysis of Proportional Methods.* Systems, 2023. **11**(4): p. 187.
9. Shen, X., et al., *An Innovative Data Integrity Verification Scheme in the Internet of Things assisted information exchange in transportation systems.* Cluster Computing, 2022. **25**(3): p. 1791-1803.
10. Sharma, S.K., et al., *Evaluation of VANETs routing protocols for data-based smart health monitoring in intelligent transportation systems.* International Journal of Mathematical, Engineering and Management Sciences, 2022. **7**(2): p. 211.
11. Gao, Z., et al., *Based on Improved NSGA-II Algorithm for Solving Time-Dependent Green Vehicle Routing Problem of Urban Waste Removal with the Consideration of Traffic Congestion: A Case Study in China.* Systems, 2023. **11**(4): p. 173.
12. Lim, K., K.M. Tuladhar, and H. Kim. *Detecting location spoofing using ADAS sensors in VANETs*. in *2019 16th IEEE annual consumer communications & networking conference (CCNC)*. 2019. IEEE.
13. Hussein, A., et al. *SDN VANETs in 5G: An architecture for resilient security services*. in *2017 Fourth International Conference on Software Defined Systems (SDS)*. 2017. IEEE.
14. Balamurugan, M., et al., *Anonymous Location-Support and Self-Reliance Routing Protocol For Manet.* Indian Journal of Public Health Research & Development, 2018. **9**(2): p. 323-326.

15. Edge, S.W., H. Cheng, and H. Zisimopoulos, *Systems and methods for 5g location support using service based interfaces*, US Patent App. 17/478, Editor. 2022, Google Patents.
16. Foundation, O.C. *Unlocking the Massive Opportunity in the Internet of Things.* [cited 2020 25 January]; Available from: https://openconnectivity.org/technology/iotivity/.
17. Hu, Q., et al., *Tangible security: Survey of methods supporting secure ad-hoc connects of edge devices with physical context.* Computers & Security, 2018. **78**: p. 281-300.
18. Appiahene, P., et al. *Application of Wireless Ad-Hoc Networks Model to provide Education to rural Communities in Ghana*. in *International Conference on Applied Science and Technology Conference Proceedings*. 2019.
19. Yang, L. and H.J.I.I.T.S. Li, *Vehicle-to-vehicle communication based on a peer-to-peer network with graph theory and consensus algorithm.* IET Intelligent Transport Systems, 2018. **13**(2): p. 280-285.
20. Bossauer, P., et al. *Trust versus Privacy: Using Connected Car Data in Peer-to-Peer Carsharing*. in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 2020.
21. Shah, S.A.A., et al., *5G for vehicular communications.* IEEE Communications Magazine, 2018. **56**(1): p. 111-117.
22. Meneguette, R.I. and A. Boukerche. *Peer-to-peer protocol for allocated resources in vehicular cloud based on V2V communication*. in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. 2017. IEEE.
23. Singh, P.K., S.K. Nandi, and S.J.V.C. Nandi, *A tutorial survey on vehicular communication state of the art, and future research directions.* Vehicular Communications, 2019. **18**: p. 100164.
24. Salem, F.M. and A.S.J.I.J.o.C.S. Ali, *SOS: Self-organized secure framework for VANET.* International Journal of Communication Systems, 2020. **33**(7): p. e4317.
25. Takashi, T., et al. *Performance Evaluation of Multi-Hop Communication on Inter-vehicular P2P Network*. in *IEICE Technical Report;*. 2020.
26. Zhang, R., Y. Lu, and B. Liu, *Pricing Decisions and Game Analysis on Advanced Delivery and Cross-Channel Return in a Dual-Channel Supply Chain System.* Systems, 2023. **11**(3): p. 155.
27. Mondal, A. and S. Mitra, *Security Issues in Vehicular* Ad Hoc *Networks for Evolution Towards Internet of Vehicles*, in *Connected Vehicles in the Internet of Things*. 2020, Springer. p. 253-307.
28. Zhong, S., et al., *Connecting things to things in physical-world: Security and privacy issues in vehicular ad-hoc networks*, in *Security and Privacy for Next-Generation Wireless Networks*. 2019, Springer. p. 101-134.
29. Stepień, K. and A. Poniszewska-Marańda. *Towards the security measures of the vehicular ad-hoc networks*. in *International Conference on Internet of Vehicles*. 2018. Springer.
30. Ayaz, S.B., et al., *Proactive route choice with real-time information: Learning and effects of network complexity and cognitive load.* Transportation Research Part C: Emerging Technologies, 2023. **149**: p. 104035.
31. Zhang, K., et al., *Artificial intelligence inspired transmission scheduling in cognitive vehicular communications and networks.* IEEE Internet of Things Journal, 2018. **6**(2): p. 1987-1997.
32. Liang, L., G.Y. Li, and W.J.I.T.o.C. Xu, *Resource allocation for D2D-enabled vehicular communications.* IEEE Transactions on Communications, 2017. **65**(7): p. 3186-3197.
33. Zhang, K., et al., *Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading.* IEEE Vehicular Technology Magazine, 2017. **12**(2): p. 36-44.
34. Burg, A., A. Chattopadhyay, and K.-Y.J.P.o.t.I. Lam, *Wireless communication and security issues for cyber–physical systems and the Internet-of-Things.* Proceedings of the IEEE, 2017. **106**(1): p. 38-60.
35. Al-Kinani, A., et al., *Optical wireless communication channel measurements and models.* IEEE Communications Surveys & Tutorials, 2018. **20**(3): p. 1939-1962.
36. Rahman, M.S., M.J.A.A. Abdel-Aty, and Prevention, *Longitudinal safety evaluation of connected vehicles' platooning on expressways.* Accident Analysis & Prevention, 2018. **117**: p. 381-391.
37. Masini, B.M., A. Bazzi, and A.J.S. Zanella, *A survey on the roadmap to mandate on board connectivity and enable V2V-based vehicular sensor networks.* Sensors, 2018. **18**(7): p. 2207.
38. Liang, L., et al., *Vehicular communications: A physical layer perspective.* IEEE Transactions on Vehicular Technology, 2017. **66**(12): p. 10647-10659.
39. Yan, G. and D.B.J.A.H.N. Rawat, *Vehicle-to-vehicle connectivity analysis for vehicular ad-hoc networks.* Ad Hoc Networks, 2017. **58**: p. 25-35.
40. Liu, G., et al., *Enhancing clustering stability in VANET: A spectral clustering based approach.* China Communications, 2020. **17**(4): p. 140-151.
41. Abdelatif, S., et al., *VANET: A novel service for predicting and disseminating vehicle traffic information.* International Journal of Communication Systems, 2020. **33**(6): p. e4288.
42. Al-Shareeda, M.A., et al., *Vppcs: Vanet-based privacy-preserving communication scheme.* IEEE Access, 2020. **8**: p. 150914-150928.
43. Xiao, H., et al., *Connectivity probability analysis for VANET freeway traffic using a cell transmission model.* IEEE Systems Journal, 2020.
44. Ali, Z.H., et al., *A novel geographically distributed architecture based on fog technology for improving Vehicular* Ad hoc *Network (VANET) performance.* Peer-to-Peer Networking and Applications, 2020. **13**(5): p. 1539-1566.

45. Khatri, S., et al., *Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges.* Peer-to-Peer Networking and Applications, 2021. **14**: p. 1778-1805.
46. Alaya, B., L.J.J.o.I.S. Sellami, and Applications, *Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks.* Journal of Information Security and Applications, 2021. **58**: p. 102779.
47. Mirsadeghi, F., et al., *A trust infrastructure based authentication method for clustered vehicular* ad hoc *networks.* Peer-to-Peer Networking and Applications, 2021. **14**: p. 2537-2553.
48. Alkhalidy, M., et al., *A new scheme for detecting malicious nodes in vehicular* ad hoc *networks based on monitoring node behavior.* Future Internet, 2022. **14**(8): p. 223.
49. Bijalwan, A., et al., *A Self-Adaptable Angular Based K-Medoid Clustering Scheme (SAACS) for Dynamic VANETs.* Electronics, 2022. **11**(19): p. 3071.
50. Ouallane, A.A., et al., *Fusion of engineering insights and emerging trends: Intelligent urban traffic management system.* Information Fusion, 2022.
51. Rajeswari, R., S.J.C. Rajesh, and Systems, *Enhance Security and Privacy in VANET Based Sensor Monitoring and Emergency Services.* Cybernetics and Systems, 2023: p. 1-22.
52. Hireche, S., A. Dennai, and B.J.T.C.J. Kadri, *Toward a Novel RESTFUL Big Data-Based Urban Traffic Incident Data Web Service for Connected Vehicles.* The Computer Journal, 2023: p. bxad001.
53. Narayanan, K.L., R.J.S.E.T. Naresh, and Assessments, *An efficient key validation mechanism with VANET in real-time cloud monitoring metrics to enhance cloud storage and security.* Sustainable Energy Technologies and Assessments, 2023. **56**: p. 102970.
54. Nazib, R.A. and S.J.I.A. Moh, *Routing Protocols for Unmanned Aerial Vehicle-Aided Vehicular* Ad Hoc *Networks: A Survey.* IEEE Access, 2020. **8**: p. 77535-77560.
55. Qureshi, K.N., et al., *Distance and signal quality aware next hop selection routing protocol for vehicular* ad hoc *networks.* Neural Computing and Applications, 2020. **32**(7): p. 2351-2364.
56. Jaiswal, R.K.J.C. and E. Engineering, *Position-based routing protocol using Kalman filter as a prediction module for vehicular* ad hoc *networks.* Computers & Electrical Engineering, 2020. **83**: p. 106599.
57. Eldin, K.Y.E. and A.A.J.J.H.e.b.e.e. Ahwal, *A Comparative Study On Vehicular Ad-Hoc Networks Topology Based Routing Protocols.* Engineering Research Journal (ERJ), 2020. **1**(44): p. 111-117.
58. Obaidat, M., et al., *Security and privacy challenges in vehicular* ad hoc *networks*, in *Connected Vehicles in the Internet of Things*. 2020, Springer. p. 223-251.
59. Sugumar, R., A. Rengarajan, and C.J.W.N. Jayakumar, *Trust based authentication technique for cluster based vehicular* ad hoc *networks (VANET).* Wireless Networks, 2018. **24**(2): p. 373-382.
60. Kolandaisamy, R., et al., *A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET.* Journal of Ambient Intelligence and Humanized Computing, 2020: p. 1-14.
61. Deshmukh, A.R., S.A. Dhawale, and S. Dorle. *Analysis of Cluster Based Routing Protocol (CBRP) for Vehicular Adhoc Network (VANet) in Real Geographic Scenario*. in *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*. 2020. IEEE.
62. Yogarayan, S., et al., *A Review of Routing Protocols for Vehicular Ad-Hoc Networks (VANETs).* 2020 8th International Conference on Information and Communication Technology (ICoICT), 2020: p. 1-7.
63. Srivastava, A., A. Prakash, and R. Tripathi, *Location based routing protocols in VANET: Issues and existing solutions.* Vehicular Communications, 2020. **23**: p. 100231.
64. Liang, L., et al., *Graph-based resource sharing in vehicular communication.* IEEE Transactions on Wireless Communications, 2018. **17**(7): p. 4579-4592.

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