An Enhance the Performance of Mining Vehicular and Machinery Security Systems Using Artificial Intelligence in VANET Cloud Computing

M. Al-Shabi

Department of Management Information System, College of Business Administration, Taibah University, 30002, Madinah Munawarrah, Saudi Arabia
E-mail: mshaby@taibahu.edu.sa

Received 18 January 2022; Accepted 13 April 2022;
Publication 05 July 2022

Abstract

Over the recent decades, incorporating Vehicular Ad-hoc Network (VANET) into Cloud computing plays a vital role, since it provides a reliable safety journey to vehicular drivers, passengers, etc. However, attaining security and emergency message dissemination is still major bottleneck in VANET combined Cloud, due to the dynamic nature of vehicles and wireless communication. Our major intention is to provide high level security in VANET-Cloud environment. In addition to it, we also reduce delay in emergency dissemination. Our proposed Delay aware Emergency Message Dissemination and Data Retrieval in secure ($DEMD^2RS$) VANET-Cloud is composed of four sequential processes: Authentication, Clustering, Data Retrieval and Data dissemination. In regard to maintaining security for both Road Side Unit (RSU) and Vehicles, we propose Hash based Credential Authentication Scheme (HCAS) that affords authentication using Secure Hash Algorithm-3 (SHA-3) and Elliptic Curve Points (ECP). To sustain a stable cluster, Firm Aware Clustering Scheme (FACS) is pursued where Stud Krill Herd (SKH) algorithm is exploited. In the data retrieval process, cloud provides

Journal of Mobile Multimedia, Vol. 18_6, 1733–1776.
doi: 10.13052/jmm1550-4646.18612

requested information to the RSU in encrypted form using the Twofish algorithm. RSU discover the path to deliver received data through executing Artificial Neural Network (ANN) algorithm. In order to diminish delay in emergency message dissemination, best disseminator is selected by cluster head using Fuzzy-Topsis (FT) algorithm. Our DEMD^{2}RS VANET-Cloud network is implemented in Network Simulator 3 tool. Finally, the evaluation of DEMD^{2}RS work performance is achieved by computing consequent metrics that are Throughput, Packet Delivery Ratio, Transmission delay, Average delay, Key generation time, Encryption time and Decryption time.

Keywords: Vehicular ad-hoc network-cloud, RSU, hash based authentication, firm aware clustering, emergency dissemination.

1 Introduction

With the success of VANET technology among vehicular consumers focuses on the excellence of comfort and realism of safety provided by this technology [1]. With the progress of technology and sudden evolvement in vehicles lead to certain issues in VANET, due to flexibility, scalability and poor connectivity. To overcome these challenges VANET is integrated into Cloud computing. Cloud provides ubiquitous services and storage to vehicular users [2]. However, maintaining security in vehicular integrated cloud network becomes difficult.

In regard to conserving security cloud based security and privacy information, dissemination scheme is introduced. Herein, Identity Based Signature (IBS) with the pseudonym method is exploited to provide authentication to the vehicles [3]. Certificate less pairing free Encryption Scheme (CCES) is introduced to provide authentication to vehicles. In this, signature based information encryption and decryption are performed where the bilinear mapping method is used to generate keys for encryption and decryption [4]. A novel geo-location based parking lock encryption mechanism is utilized to provide the security in VANET-Cloud environment for location privacy and non-frameability [5]. In this, the Traffic Management Bureau (TMB) Clustering of vehicles in the VANET environment reduces the high mobility of vehicles. The analytical model is utilized to cluster the vehicles in the network [6].

Link Reliability based Clustering Algorithm (LRCA) is exploited to provide efficient and reliable message transmission in VANET. LRCA based

clustering performs, cluster head selection, cluster formation and cluster maintenance processes. Redundant unstable neighbours are filtered out using Link Lifetime based sampling method [7]. Mobility Prediction based Efficient Clustering Scheme (MPECS) is used in VANET where network regions are split through Voronoi diagram by using main intersections as centers of partitioned area. Using MPECS, each vehicle can predict its own longevity and cost for electing as cluster head [8]. Weighted K-Medoid based Clustering approach is utilized to form clusters in vehicular network. In weighted K-Medoid clustering, hybrid genetic algorithm is used to maintain the clusters where Tabu search is incorporated into genetic algorithm [9].

Sampling based Estimation Scheme (SES) is introduced to route the packets from source to destination. SES method finds path using probabilistic contacts on overlapped road into multiple segments as samples. Each sample provides possible routing decision [10]. Bilateral Forwarder Determination method scheme is used to find best forwarder determination. Bilateral Forwarder method includes both Inter community forwarder determination and Intra community forwarder determination [11]. Hybrid relay selection scheme is used to disseminate emergency message among vehicles in VANET. Hybrid scheme considers spatial distribution of next hop node with reference to the sending node. This relay selection scheme uses multiple criteria based relay selection scheme to select group of relay nodes [12].

An adaptive data dissemination protocol based emergency dissemination is proposed in vehicular network. This protocol proposes different mechanism to dynamically adjust the beacon intervals [13]. Novel Store and Carry Forward scheme based message dissemination is introduced in VANET. Here, SCF enable vehicles only forwards emergency message to the neighbour vehicles [14]. Time barrier based emergency dissemination scheme is introduced in vehicular network. Herein, super node is selected initially in order to disseminate the emergency message. In this, time barrier method, super node disseminate emergency message to the neighbour vehicles in timely manner [15]. Multi-channel coordination scheme is introduced for emergency dissemination in VANET. Multi-channel coordinator selection process is achieved using Least Average separation Distance (LAD) to the vehicles where control channel is used for emergency dissemination [16].

From the above listed works, we have noticed that still there exist issues in VANET-Cloud environment. The issues are summarized as follows:

- Providing security in VANET-Cloud environment is difficult due to the frequent topology changes.

- Cluster formation in VANET-Cloud environment is difficult due to the high mobility of the vehicle.
- Security is a major constraint in routing since most of the works doesn't concentrated on secure data transmission
- Delay is high in emergency dissemination due to lack of parameter consideration in disseminator selection.

1.1 Our Motivation

This section deals with the motivation with research gaps in the VANET-Cloud environment. Integration of VANET into Cloud environment provides ubiquitous advantages to the users in terms of the high level of infotainment information storage and faster response to the user request.

Most of the works presented in the VANET-Cloud environment provides security by authenticating vehicles only. However, there is also a chance to deploy malicious RSU on the roadsides. As yet, there is a research gap in authenticating RSU in order to provide high level security to VANET-Cloud communication. And also, there is a lack in providing security to the user credentials stored in the cloud. Furthermore, reducing delay in emergency dissemination is difficult due to frequent link losses. In addition, most of the emergency dissemination works doesn't considered the delay in emergency dissemination. It is also a major research gap in the VANET-Cloud environment. Forming stable clusters and secure data transmission in VANET-cloud environment is a big issue due to the high mobility and lack of data security.

Our DEMD^{2}RS work resolves the aforesaid research gap in the DEMD^{2}RS VANET-Cloud network effectually. By solving these research gaps, our work differs from the other existing works performed in the VANET-Cloud environment. In our work, we provide authentication to the both RSU and vehicle in order to provide high level security to the VANET-cloud communication. In addition to it, we also provide security to the user credentials by splitting cloud server into two types. Our work reduces delay in emergency dissemination via considering effective parameters and algorithms for disseminator selection. We also form stable clusters in the VANET-Cloud network with secure data transmission using an effective cryptography algorithm.

1.2 Our Contributions

The core contribution of this work is twofold: Our work provides high level security to the user credentials and also provides secure data transmission in

order to secure data from the malicious users. And also reduces the delay in disseminating the emergency message in VANET-Cloud environment.

- To ensure the security of the user credentials, we split the cloud server into two that are: Data Server (DS) and Meta Data Server (MDS). MDS establishes high security to user credentials and DS stores encrypted data.
- Security in Cloud enabled VANET is conserved through two mechanisms: First is to provide authentication which is carried out using HCAS where the SHA-3 algorithm is employed to authenticate RSU and Vehicles. The second is to provide secure data transmission for which Twofish algorithm is used.
- In order to reduce frequent clustering process, DEMD^{2}RS work establishes FACS based clustering where subsequent metrics are considered such as velocity, direction, node degree, node connectivity, stability factor and lifetime of the vehicle.
- ANN based routing is performed to transmit data in a secure way where following metrics are taken namely velocity, direction, trust value, the expected number of transmission count, distance and expected number of transmission time.
- In regard to disseminate emergency messages timely, DEMD^{2}RS work utilizes best disseminator selection in each cluster by cluster head. Cluster head selects the best disseminator using the FT algorithm.

1.3 Organization of This Paper

The rest of this paper is structured as follows. Section 2 summarizes the related work regarding emergency message dissemination in VANET-Cloud environment. Section 3 explains the problems that are exist in the present VANET-Cloud emergency dissemination. Section 4 describes briefly about DEMD^{2}RS delay aware emergency dissemination and data retrieval in VANET-Cloud. Section 5 highlights experimental results of DEMD^{2}RS work. Section 6 concludes contribution of this work and comments with some future directions.

2 Related Work

In this section, we review works that are related to the proposed system associated with the secure VANET-Cloud, clustering, routing and emergency

dissemination. A number of current studies explained and devised mechanism for secure combination of VANET and Cloud.

2.1 Secure VANET-Cloud

This section discusses the works that are related to the secure VANET-Cloud environment. Kai et al. [17] have proposed secure and efficient privacy preserving cipher-text retrieval in connected vehicular cloud computing. Herein, cipher text based search system is implemented to exploit RSU as super peers for connected vehicular cloud computing. In this framework, all the computations and retrieval operations are handled by the super peers. In connected vehicular cloud computing, user documents are stored in the cloud to provide better security and high efficiency. Data retrieved vehicles get keys from source vehicles to decrypt the encrypted data. Herein, data are not stored securely while data index are stored in Hash form using SHA-1 algorithm that has less security compared to other SHA algorithm.

Yixian et al. [18] have proposed secure and efficient transmission method in connected vehicular cloud computing. The proposed connected vehicular cloud computing that extends the fixed node of the traditional cloud to the mobile nodes. In this novel computation approach is proposed to find the channel capacities of the multiple vehicular networks. Herein, secure and efficient transmission is achieves through game theory and information theory. Nash equilibrium is executed in game theory in order to obtain optimal results. Cloud only sends emergency information to vehicles that are nearby accidental zone. This paper doesn't follow any security mechanism to ensure security of the stored information in cloud.

Hamssa et al. [19] have proposed trust model for secure group leader based communication in vehicular environment. The proposed work consists of Hybrid Trust Model (HTM) and Misbehavior Detection System (MDS). These systems are used to provide trust metric to each vehicle based on its behaviour. Using this metric this paper classifies the malicious from the normal nodes. The back end system is used to select the optimum group leader based on the higher trustworthiness. This work evaluates trust based on behaviour that doesn't consider necessary metrics related to the misbehavior detection system.

Abderrahim et al. [20] have proposed security scheme in vehicular cloud network through lightweight encryption algorithm. Herein, each vehicular cloud users receives smart card by the vehicular cloud infrastructure, in order to verify the authentication of vehicle user. Message Digest algorithm

Table 1 Merits and demerits of the secure VANET-Cloud works

References	Merits	Demerits
Kai et al. [17]	High Robustness in securing data	Security is provided only to the data index that tends to forging of data
Yixian et al. [18]	High reliability in securing cloud data	Security is doesn't provided to the cloud data
Hamssa et al. [19]	Consumes less time in predicting malicious users	Absence of significant credentials consideration leads to poor security mechanism
Abderrahim et al. [20]	Introduces lightweight securing mechanism	Smart card based authentication is used which is easily forgeable

is used to generate hash values for user registered credentials such as ID, vehicle registration numbers. Authentication process execution is depends on the random number generated. Since, random numbers are generated at the time user registrations are integrated with the generated hash value by the vehicular cloud infrastructure. These credentials are verified in authentication process along with smart card. This paper uses smart card for authentication process that can be easily forged by the malicious users. Table 1 describes the merits and demerits of the Secure VANET-Cloud works.

2.2 Clustering

This portion discusses the works that are related to the clustering the vehicular cloud network. Lei et al. [21] have proposed clustering and probabilistic broadcasting using data dissemination scheme in VANET. In this, clusters are formed based on the direction of driving vehicles. Using clusters each vehicle can transmit their data to the neighbor vehicle where cluster head is selected using link connectivity and packet successful transmission probability. Probabilistic forwarding approach is proposed to disseminate the data among the vehicles. Each cluster member forwards the received packet to its cluster head along with the computed probability that is associated with the number of times the same packet is received during one interval. Neighbours are discovered by broadcasting periodical beacons to its neighbours. Cluster head is selected based on two factors only which are not sufficient to form effective cluster in VANET environment.

Sarah et al. [22] have proposed secure and stable clustering algorithm based on hybrid mobility of vehicles and trust management scheme. New approach is proposed for trustworthy cluster head selection where stability

and trust factors are considered. In trust management scheme, trust of data that can be changed between vehicles and communication capabilities. In cluster formation step, each vehicle exchange hello packets that contain ID, speed, acceleration and position. Cluster head is elected based on the computation of score where mobility metrics are considered. This work doesn't focus on security parameters in order to maintain security in vehicular environment.

Yasir et al. [23] have proposed Moth Flame Optimization (MFO) based clustering algorithm in VANET. In this work, clustering is performed using efficient clustering algorithm MFO which forms the clusters effectively. At first, network of the autonomous vehicles are generated by the randomly initialized their position with its respective region. The fitness function is calculated using the position of the moths in searching space. Based on the highest fitness function cluster head is selected in the network. Cluster head selection is not effective, because it considers two metrics only such as distance and speed.

Yassine et al. [24] have proposed new communication model for VANET environment. New communication model considers road as a ring segment. New communication model forms clusters in order to maintain the stable routes during inter cluster communication. In cluster head selection, candidate vehicle broadcast hello message that contains ideal position and mobility metrics. Each vehicle provides vote to the neighbor vehicles based on probability value and ideal location. If there is no vehicle present in the ideal position, then vehicle near to the ideal position is selected for aggregation. Cluster head selection is based on the voting, there may chances to select non-optimal vehicle as cluster head. Table 2 describes the merits and demerits of the clustering works.

2.3 Routing

This part deals with works that are associated with the routing in vehicular cloud network. Hui et al. [25] have proposed novel trust based multicast routing for VANET. The proposed model computes two trust factors that include direct and indirect trust. The direct trust is computed based on the Bayesian theory and in-directed trust is computed based on the evaluation credibility and activity. The fuzzy logic approach is used to discover the direct and indirect trust values. The total trust values of the nodes are obtained using Defuzzification process. Based on the computed trust value efficient routes are selected to transmit the data delivery. This paper finds route based on the trust factor only that leads to loss in transmitted packet.

Table 2 Merits and demerits of the clustering works

References	Merits	Demerits
Lei et al. [21]	Effective data transmission	Cluster head selection is not effective due to lack of parameter consideration
Sarah et al. [22]	Considers QoS parameters while forming clusters that enhances the system performance	Consumes more bandwidth while selecting cluster head
Yasir et al. [23]	Consumes less time to form clusters	MFO based cluster head selection cannot able to select an optimal head due to poor convergence
Yassine et al. [24]	Less process to form clusters in the network	Frequent formation of cluster due to ineffective head selection

Table 3 Merits and demerits of the routing

References	Merits	Demerits
Hui et al. [25]	Increases scalability in data transmission	Transmission loss is occur while routing packet to the destination
Sha et al. [26]	High reliable data transmission	Lack of parameter consideration in routing induces packet losses

Sha et al. [26] have proposed delay aware relay selection in vehicular network. This paper proposes Greedy Parameter Stateless Routing (GPSR) based routing protocol for data dissemination in the heterogeneous communication range. The neighbour table with asymmetric wirelength is established with the help of acknowledgement list and intermediate nodes. The vehicle with minimum expected transmission delay is selected as the next hop for the transmission. The expected transmission delay is combination of the expect delay and communication range. This factor is used to estimate the delay from the current packet carrying vehicle to destination. Relay node is selected based on the delay factor; hence the routing is not effective in terms of transmission loss. Table 3 describes the merits and demerits of the routing works.

2.4 Emergency Data Dissemination

This section describes the works that are related to the emergency dissemination in vehicular network. Li et al. [27] have proposed reliable emergency message dissemination protocol for vehicular network. The proposed protocol consists of layout aware ready to broadcast and clear to broadcast

Table 4 Merits and demerits of the emergency dissemination works

References	Merits	Demerits
Li et al. [27]	Improves reliability in emergency data transmission	Broadcasting the emergency message induces broadcast storm
Daxin et al. [28]	Consumes less time to select disseminator	Delay is high while disseminating emergency message
Yusor et al. [29]	Increase scalability of the system	Emergency message dissemination is not effective due to lack of delay oriented par

message handoff mechanism and redundant relay node adaptation mechanism. The emergency message broadcast is based on the two phases that are intersection broadcast process and road segment broadcast process. The back off timers is set to the relay nodes to avoid overlap in time so that replies do not collide. By receiving last clear to broadcast message, the data message transmission is commenced. Broadcast message based dissemination leads to more delay in emergency message dissemination.

Daxin et al. [28] have proposed distributed position based protocol for emergency message broadcasting in VANET. Herein, improved position based protocol is proposed to disseminate the emergency message among large scale vehicular networks. Using the proposed protocol emergency messages are only broadcasted to the interested region and rebroadcast of the messages is depends on the information included in the message. Yusor et al. [29] have proposed accident management system based on vehicular network for intelligent transport system. Accident management system consists of three modules that are sensor module, speed monitor module and message and alert module. Herein, sensor module is used to monitor and control the sensors deployed in the network. Message and alert module is used to maintain the communication between RSU unit, ambulance and central server. Speed monitor module is used to measure the speed of each vehicle. Author discussed in [28] and [29] have more delay in emergency message dissemination, since it considered delay oriented factors in emergency message dissemination. Table 4 describes the merits and demerits of the clustering works.

3 Problem Statements

In this section, we designate the problems that are present in the existing VANET-Cloud network. We have identified the major problems in the existing works that are listed as follows:

- Lack of credentials consideration during authentication of the vehicles that tends to easy forgeable of the cloud stored data by malicious users.
- Formation of stable clusters in VANET-Cloud environment is difficult due to frequent link losses among vehicles.
- An optimal forwarder selection is difficult due to the usage of ineffective algorithms. As a result, delay is increased in emergency dissemination.
- Transmission delay and losses are more while routing packets to the destination.

We have also identified problems in the individual works performed in the VANET-Cloud environment that are discussed as below:

Secure and reliable communication based data transmission is introduced in vehicular cloud environment [30, 31]. Herein, vehicles are authenticated using gateways which are not secured, because gateway itself can be malicious. In addition, ID and Password is used for authentication, it can be easily forgeable by the malicious users. Blowfish based encryption method is not effective since it suffers in large network environment. Cluster based Emergency Message Dissemination (CEMD) in VANET [32]. Herein, Cluster formation is not effective, because it considers only average speed of the vehicle not direction. Emergency message broadcast increases delay, since source node waits for CTB message before disseminating the emergency message. Hidden Markov Model (HMM) based routing is established in vehicular cloud network [33]. In HMM node insertion and deletion operations are difficult that tends to increase the delay in transmission and also increases the packet loss. A trust worthiness evaluation based routing protocol is suggested for vehicular network [34]. Here, route selection is not effective, since it selects the forwarder using PCA which doesn't compute trust value effectively due to high variance in the attributes. Adaptive Emergency Broadcast Strategy (AEBS) is introduced for VANET-Cloud network [35]. Stability based forwarder selection is not effective because it considers only distance and relative velocity that tends to increase the delay in emergency message broadcasting. To overthrow aforementioned issues, we propose "Delay aware Emergency Dissemination and Data retrieval in secure VANET-Cloud environment".

4 System Model

4.1 Network Overview

Emergency message dissemination service is the essential application in Cloud assisted VANET architecture. An efficient mechanism is needed for

emergency dissemination and also secure data retrieval in VANET-Cloud environment. Figure 1 depicts the architecture for DEMD^{2}RS work where vehicles (V_1, V_2 ... V_n), RSU (R_1, R_1 ... R_n), Trusted Authority (TA) and Cloud servers (Data servers and Meta data servers) are signified. Our DEMD^{2}RS method contributions are four fold: Authentication, Clustering, Data retrieval and Data dissemination. Our DEMD^{2}RS cloud environment has two servers namely Data Server (DS) and Meta Data Server (MDS). TA authenticates vehicles and RSU, in order to provide secure VANET-Cloud where HCAS is proposed. After completing authentication, user credentials are stored in MDS and other data like parking information, weather information, etc. are stored in DS. FACS is proposed to form clusters using SKH algorithm. During data retrieval process, user credentials are verified and cloud provides encrypted data to the RSU where encryption is executed using Twofish algorithm which is highly secure. RSU sends encrypted data to the destination vehicle through optimum path which is selected using ANN algorithm. Data dissemination process, optimum disseminator is chosen to reduce delay in emergency message dissemination. Herein, FT algorithm used which considers succeeding metrics to select best disseminator that are forwarding probability, delivery delay, mobility and node degree.

4.2 Definition of System Model

Our DEMD^{2}RS work has four entities that are explained as follows:

(i) TA

TA is trusted third party which is responsible for authentication vehicle users and RSU, in order to provide security to the user's credentials and stored data in cloud.

(ii) RSU

RSU is a road side unit deployed to provide easy access communication between vehicles and cloud servers.

(iii) Cloud servers

Cloud servers are responsible for storing mass amount of data that are useful for safety journey of vehicles. In our work, we split cloud sever into DS and MDS. DS contains encrypted information about weather, parking, etc. Whereas MDS contains secret credentials of vehicles users and RSUs, since these informations are highly confidential.

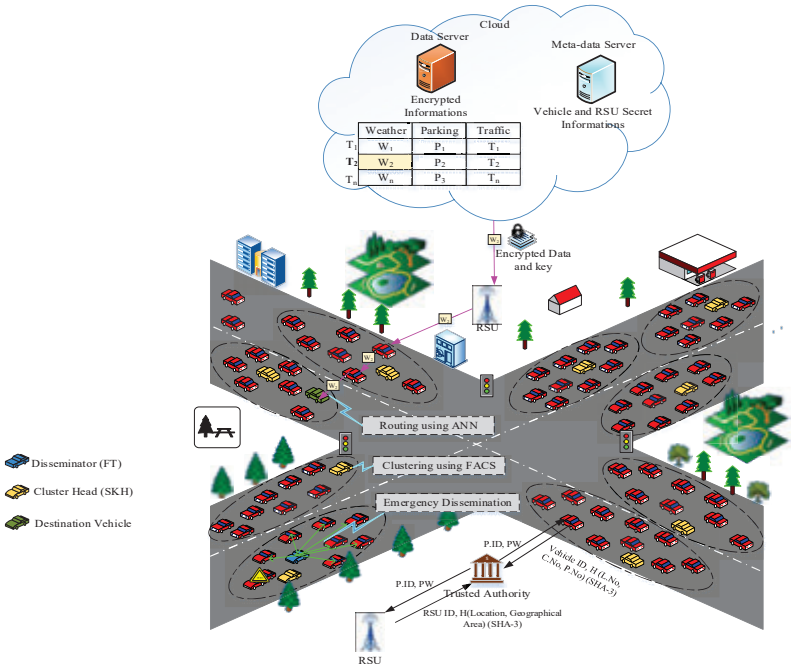

Figure 1 Architecture for DEMD^{2}RS Work.

MDS provides high security to the stored data; hence we store confidential information in MDS.

(iv) Vehicle

Vehicles are moving objects in the road that gather informations from the cloud server through RSU, supposed to maintain safety journey.

4.3 Authentication

Authentication is one the significant process in our DEMD^{2}RS secure cloud assisted VANET. TA is used to authenticate both RSUs and Vehicles. Authentication avoids malicious user's access in cloud stored data and also provides high level security to the stored data.

4.3.1 Vehicle registration and authentication

Vehicles are sending registration request to the TA along with vehicle ID and hash values of Plate Number (P. No), License Number (L. No), Chassis

Number (C. No). Hash values are generated using SHA-3 algorithm. Herein, L. No and P. No are provided by the government authority whereas C. No is provided by the car manufacturer. RSU sending registration request to the TA along with RSU ID and hash values of location and geographical area.

$$V_i \rightarrow v.ID, \quad H_{P.\ No}, H_{C.No}, \quad H_{L.No} \rightarrow TA \tag{1}$$

Where, hash values are generated using SHA-3 algorithm. Herein, SHA-3 takes input as plain text and converts it into hash value. SHA-3 uses Keccak sponge construction where data are absorbed into the sponged and squeezed out as result which is hash value. Proposed SHA-3 algorithm provides better security than SHA-2 and 1 version. Cycles used also reduced compared to the other SHA algorithm, since it requires 24 cycles to generate hash values for given input. Usually, a strengthen hash function has following properties that are,

(1) One way Property:

For a given value h, it should be very difficult to find any message 'g' that is expressed as,

$$\mathrm{h} = \mathrm{hash}\ (\mathrm{g}) \tag{2}$$

(2) Weak Collision Resistance:

For a given input g_1, it should be difficult to find different g_2 that can be expressed as follows,

$$\mathrm{hash}(\mathrm{g}_1) = \mathrm{hash}(\mathrm{g}_2) \tag{3}$$

(3) Strong Collision Resistance:

For a given input, it should be difficult to find two different messages g_1 and g_2,

$$\mathrm{hash}(\mathrm{g}_1) = \mathrm{hash}(\mathrm{g}_2) \tag{4}$$

SHA algorithms such as SHA-0, SHA-1, SHA-2 and SHA-3 cryptography algorithms are established by NIST standard.

Hash values for P. No, C. No and L. No are generated as follows,

$$H_{P.No} \rightarrow h(P.No) \tag{5}$$

$$H_{C.No} \rightarrow h(C.No) \tag{6}$$

$$H_{L.No} \rightarrow h(L.NO) \tag{7}$$

Above equation represents the hash values of plate, chassis and License numbers. Herein, we consider last four digits of C. No, typically C. No has twelve digits. These credentials transmitted to TA for registration purpose.

After getting credentials from the vehicle users, TA generates pseudo ID and password. In this, pseudo ID is generated using ECP which is unique for each vehicle [36]. Let us consider, elliptic curve $\mathbb{E}$ over the binary field $\mathbb{F}_{2^l}$ which is defined by the below equation,

$$y^2 + xy = x^3 + ux^2 + w \tag{8}$$

Where, parameters $u, w \epsilon (\mathbb{F}_{2^l})$ with $w \neq 0$. The set $\mathbb{E}(\mathbb{F}_{2^l})$ consists of all points of (x, y), $x \epsilon \mathbb{F}_{2^l}$, $y \epsilon \mathbb{F}_{2^l}$ which satisfies the above equation together with a special point '$\mathcal{O}$' which is called the point at infinity. Herein, field $\mathbb{F}_{2^l}$ called characteristic two finite field or binary finite field. It can be viewed as a vector space of dimension 'l' over the field $\mathbb{F}_{2^l}$ where two elements are exists i.e. $\{0, 1\}$. In this variables x and y and co-efficient 'u' and 'w' are elements of the finite field $\mathbb{F}_{2^l}$.

Pseudo ID generated using elliptic points are given as follows,

$$P.ID_V = i\,(1 + h_i) + U_0 \tag{9}$$

Where, h_i is random bits resides $h_i \epsilon \{0, 1\}$ and $i = 0, 1, \ldots n$. Herein, $U_0(x, y)$ represents the initial value resides in $U_0(x, y) \in \mathbb{F}_{2^l}$. After completing computation of Pseudo ID, TA concatenates last four digits of hash values generated for P. No, C. No and L. No to generate password which is expressed as follows,

$$PW_V = H_{P.No} \| H_{C.No} \| H_{L.No} \tag{10}$$

Finally, TA provides generated Pseudo ID and Password to the vehicle user which is expressed as follows,

$$TA \rightarrow P.ID_V, \quad PW_V \rightarrow V_i \tag{11}$$

4.3.2 RSU registration and authentication

RSU registration process executed similarly like vehicle registration. RSU sends registration request to TA along with credentials such as RSU ID and hash values of geographical area and location.

$$R_i \rightarrow R.ID, \quad H_{GA}, \quad H_L \rightarrow TA \tag{12}$$

Herein, hash of geographical area and location is computed using SHA-3 as computed in vehicle registration. Hash values are generated using following expression,

$$H_{GA} = h(GA) \tag{13}$$

$$H_L = h(L) \tag{14}$$

After completing hash generation for credentials, RSU sends it to the TA along with RSU ID. After receiving credentials from RSU, TA generates Pseudo ID and Password. Herein, Pseudo ID is generated using ECP as generated during vehicle registration. Pseudo ID is generated using below equation,

$$P.ID_R = j(1 + h_j) + Q_0 \tag{15}$$

Where, h_j is random bits resides $h_j \epsilon \{0, 1\}$ and $j = 0, 1, \ldots n$. Herein, $Q_0(x, y)$ denotes the initial value belongs in $U_0(x, y) \in \mathbb{F}_{2^l}$. After completing computation of Pseudo ID, TA concatenates last four digits of hash values generated for P. No, C. No and L. No to generate password which is expressed as follows,

$$PW_R = H_{GA} \parallel H_L \tag{16}$$

Finally, TA provides generated Pseudo ID and Password to the RSU which is expressed as follows,

$$TA \rightarrow P.ID_R, \quad PW_R \rightarrow V_i \tag{17}$$

4.4 Clustering

Clustering is essential process in VANET integrated Cloud environment. Vehicles are moving dynamically in road; hence forming stable cluster in vehicular environment is tricky. To address this issue, we propose stable cluster formation using FACS. FACS consists of two processes that are Cluster Head (CH) selection and Cluster formation. CH selection is achieved through SKH algorithm [37]. SKH consider each individual vehicle (V_1, V_2 $\ldots V_n$) as krill ($k_1, k_2, \ldots k_n$).

4.4.1 CH election

CH election carried out using SKH which considers subsequent metrics for instance direction, velocity, Node degree, Node connectivity, stability factor and lifetime of the vehicle. These metrics are explained as follows,

(a) Direction

Direction metric is used to find the vehicle moving direction that is highly important while selecting CH.

(b) Velocity

Velocity is the vehicle moving speed with respect to the time which is also important, in order to reduce frequent election of cluster head. Velocity of the vehicle is computed using following expression,

$$v_i = \frac{d_i}{t_i} \tag{18}$$

Here, d_i represents distance moved by the vehicle 'i' at time 't_i'.

(c) Node degree

Node degree metric plays vital role in cluster formation, since node which has highest number of neighbor can easily communicate with other. It can be expressed as follows,

$$ND_i = |N_{c,i}| \tag{19}$$

Here, $|N_{c,i}|$ represents neighbour count of the vehicle 'i'.

(d) Node Connectivity

Node connectivity is important to consider, in regard to provide better transmission among cluster member nodes. It defines relative position difference between vehicles 'i' and 'j'. Node connectivity metric is expressed as follows,

$$NC_i = |V_i - V_j| \tag{20}$$

Here, V_i and V_j represents position of vehicle 'i' and 'j'.

(e) Stability Factor

Stability factor is defined as the speed difference between ith vehicle and its neighbour vehicle. It can be expressed as follows,

$$sf_i = 1 - \frac{\mathrm{V}_{d,i}}{\mathrm{V}_{max}} \tag{21}$$

Here, $\mathrm{V}_{d,i}$ represents average speed of vehicle 'i' and nearby vehicle. V_{max} represents maximum speed of the vehicle.

(f) Lifetime of the vehicle

Lifetime of the vehicle is used to measure how much time, it resides in particular cluster that leads to maintain steady cluster.

By utilizing aforementioned metrics SKH algorithm computes fitness function to select optimum CH. The proposed SKH algorithm is one of the metaheuristic algorithms which is inspired by the biological behaviour of swarms. Herein, krill positions are updated through Stud Selection and Crossover (SSC) operator that provides fast convergence. SSC operator is employed to tune the selected solution, in order to enhance its consistency and also robustness for global optimization. SKH algorithm inspired by the succeeding activities such as,

(i) Displacement stimulated by the different krill
(ii) Foraging Motion
(iii) Physical Diffusion

Fitness function for each individual krill is computed as follows,

$$F(k_i) = \sum_{i=0}^{n} \left(\frac{1}{(d_i + v_i + sf_i)} + (ND_i + NC_i + LT_i) \right) \tag{22}$$

Above fitness computation is performed for each individual krill, in regard to perform SSC operations. After completion of fitness function computation, SSC operator performs Mutation and Crossover functions, in order to select best CH.

(a) Crossover

Crossover operation is performed to combine characteristics of two krill's in order to generate new krill. Crossover operation is expressed as follows,

$$k_{i,m} = \begin{cases} k_{r,m} & rand_{i,m} < C_r \\ k_{i,m} & else \end{cases} \tag{23}$$

Where, $C_r = 0.2\ k_{best}$ and $r \in 1, 2, \ldots i-1, i+1, \ldots n$.

(b) Mutation

Mutation operation is performed to maintain the diversity of the one generation of population to the next generation. It can be expressed as follows,

$$k_{i,m} = \begin{cases} k_{gbest,m} + \mu(k_{p,m} - k_{q,m}) & rand_{i,m} < \tau \\ k_{i,m} & else \end{cases} \tag{24}$$

Where, $\tau = \frac{0.05}{k_{best}}$ and $k_{gbest,m}$ denotes the global best krill node. $p, q \in 1, 2, \ldots i-1, i+1, \ldots n$.

After completion of above two operations, SKH compares fitness of k_i and k_j. If k_j is greater than k_i, then k_j is fixed as global best or else krill position is updated. This process is functioned until maximum iteration reached.

Algorithm for CH election

Input: $d_i, v_i, sf_i, ND_i, NC_i, LT_i$
Output: Best CH selected
Begin

1. Define parameters population size n and maximum iteration count I.
2. Initialize population k_i of n krill individual, forging speed, diffusion speed and probability of crossover.
3. Evaluate fitness function using Equation (22) for each individual krill.
4. For each individual Krill
   - 4.1. Perform three activities (Displacement stimulated by the different krill, Foraging Motion and Physical Diffusion)
   - 4.2. Implement SSC operations
   - 4.3. Compute fitness function according to new position
5. Update fitness function for each krill
6. Repeat step 4 and 5 until stopping criteria reached
7. Select best CH

Above algorithm describes the CH election performed by SKH algorithm. At first, population size and maximum iteration count are defined and initialization process is performed. Fitness function is computed using equ to find global best krill. SSC operations are performed to generate new krill and compute new fitness for each krill and it is updated. These processes are repeated until stopping criteria reached. Finally, optimum CH is selected using SKH algorithm effectually.

4.4.2 Cluster formation

Cluster formation is performed after completion of CH election. Herein, CH forms cluster based on the average speed and node degree of the neighbor vehicle according to sustain firm cluster. In this, average speed of the vehicle is computed using following expression,

$$AS(i,x) = \frac{S_x + S_i}{2} \tag{25}$$

Where, S_x represents speed of CH and S_i represents speed of neighbour vehicle. Node degree is computed using equ. to select highest node degree vehicle that provide better communication with other vehicles. Vehicle with less average speed and high node degree is selected as cluster member by CH. This process is performed for all nearby vehicles to form constant cluster.

4.5 Data Retrieval

Data retrieval process is divided into encryption and routing process. Encryption process is executed using Twofish algorithm and Routing process is executed through ANN algorithm.

Vehicle that requires informations about road condition, traffic jam, etc. sends data retrieval request to the CH along with Pseudo ID and Password. After receiving request from cluster member, CH sends request to Cloud server via RSU. Cloud server verifies received credentials and provides requested data in encrypted form. Here, encryption is performed using Twofish algorithm which is highly secure compared to the other algorithm [38]. Here, Twofish algorithm is used to encrypt the data that are stored in the cloud server in order to secure data transmission.

Figure 2 illustrates the encryption of plain text using Twofish algorithm. Twofish is symmetric key cryptography algorithm which has 128 bit

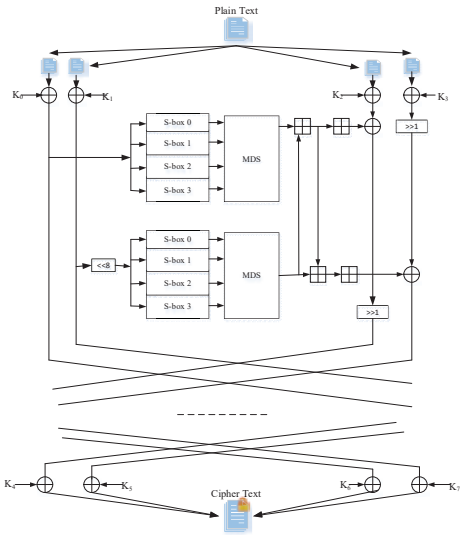

Figure 2 Twofish encryption.

symmetric block size and key length as 128, 192 and 256 bits with 16 rounds. Twofish algorithm doesn't contain any weak keys. Twofish algorithm has four entities that are S-boxes, MDS matrix, Pseudo-Hadamard Transforms (PHT) and whitening. Herein, S-boxes are substitution box which is used to perform substitution operation. MDS matrix is used to diffuse the output from the S-boxes. At first, given plain text input of 16 bytes p_0, $p_1 \ldots p_{15}$ are spilt into the four words which is defined in following expression,

$$p_i = \sum_{j=0}^{3} p(4i + j) \cdot 2^{8J} \tag{26}$$

Where, i = 0, 1, 2, 3. After completion of splitting of words, input whitening process is performed which is explained as below expression,

$$R_{0,i} = P_i \bigoplus K_i \tag{27}$$

Where P_i represents the plain text and K_i represents key. After completion of input whitening, MDS matrix output are given to the PHT. PHT is used to mix the output from the MDS matrices. For a given input 'a' and 'b', PHT is defined by,

$$a' = a + b \; mod \; 2^{32} \tag{28}$$

$$b' = a + 2b \; mod \; 2^{32} \tag{29}$$

Whitening process is performed in both input and output sides of the encryption. Whitening is used to increase the security of the iterative block cipher. Output whitening process is performed as follows,

$$C_i = R_{16,(i+2)mod\ 4} \bigoplus K_i \tag{30}$$

Where, C_i represent the cipher text of the given plain text P_i. By utilizing above expressions, raw data is converted into the encrypted data. Cloud sends encrypted data along with key to the destination vehicle via RSU. RSU finds routes using ANN algorithm which performs fast and selects optimum path to transmit data to the destination. For route selection, we consider succeeding metrics that are velocity, direction, trust value, expected number of transmission count, distance and expected transmission time.

(i) Trust Value

Trust value metric is significant to compute to discover highly trusted vehicle. Trust value is computed using following expression, in order to maintain the

security and reduce loss in transmission. It can be expressed as follows,

$$TV = \sum \frac{1}{P_L + B_s} \tag{31}$$

Where, P_L denotes packet loss induced by the vehicle and B_s denotes buffer size of the vehicle. We consider these two metric in order to find malicious vehicle, since malicious vehicle has high packet loss and buffer size.

(ii) Distance

Distance metric is used to measure the vehicle is how much distance from the destination vehicle. Distance metric is computed to reduce delay in routing. It can be expressed as follows,

$$D_{i,d} = \sqrt{(v_{d,x_1} - v_{i,x_1})^2 - (v_{d,y_1} - v_{i,y_1})^2} \tag{32}$$

Where, v_{d,x_1}, v_{d,y_1} represents x and y position of destination vehicle. v_{i,x_1}, v_{i,y_1} denotes x and y position of ith vehicle.

(iii) Expected Transmission Count

Expected Transmission count metric is used to measure quality of the link between the destination vehicle and packet transmitted vehicle to provide packet without any error. It can be expressed as follows,

$$ET_c = \frac{1}{NL_Q * L_q} \tag{33}$$

Where, NL_Q represents neighbour link quality and L_Q represents link quality.

(iv) Expected Transmission Time

Expected Transmission Time metric is defined as the time required to transmit given packet to the destination which is also reduce delay in routing. It can be expressed as follows,

$$ET_T = ET_c * \frac{P_s}{L_c} \tag{34}$$

Where, P_s denotes packet size, L_c denotes link capacity and ET_c denotes expected transmission count.

By utilizing above metrics, ANN computes weights for vehicles to transmit encrypted data to the destination. Let us consider 'N' be a neural network with 'e' connection, 'i' input and 'o' output. ANN considers each input node as vehicular node from which it takes aforementioned metrics to compute weights in hidden layer. Weight computation of ANN is accomplished via stochastic gradient method. Weight computed in hidden layer by applying stochastic gradient is expressed as follows,

$$\mathrm{w}_i = \sum_{i=0}^{n} \delta \left[d_i + v_i + TV + ET_c + \left(\frac{1}{ET_T + D_{i,d}} \right) \right] + \varepsilon(t) \tag{35}$$

Where, δ represents the learning rate and $\varepsilon(t)$ denotes the stochastic term. After completing computation of weight for each vehicle in hidden layer, output layer provides output. Output for given input in ANN is expressed as follows,

$$\mathrm{y} = f_n(\mathrm{w}_i, x) \tag{36}$$

Above expression explains for a given input x, computes weights which maps into the respective output 'y'. Vehicles having highest weight only selected to forward the encrypted data to the destination node without delay and transmission loss.

Figure 3 demonstrates the ANN based weight computation where vehicle with highest weight only selected to forward encrypt data to the destination.

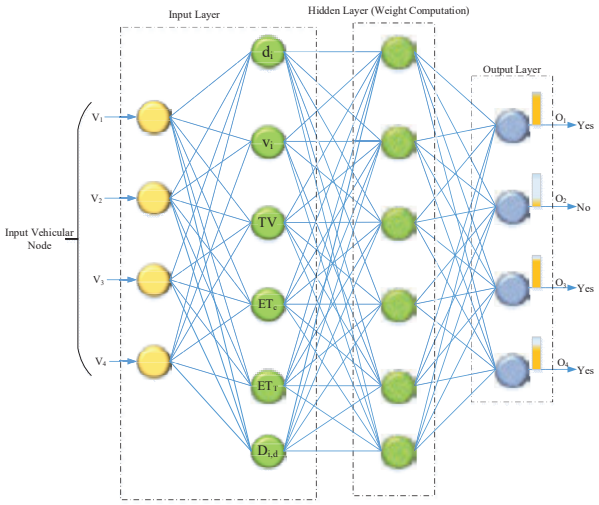

Figure 3 ANN based weight computation.

ANN provides output in yes or no format where yes indicate vehicle has high weight and no indicates vehicle has low weight. By utilizing ANN based routing, our proposed method achieves less transmission loss and less delay.

4.6 Data Dissemination

Data dissemination is final process in our DEMD^{2}RS work where best disseminator is selected. Best disseminator is selection process executed through CH where FT algorithm. If any accident occurs, then selected disseminator disseminate emergency message to its cluster member that reduce collision and broadcast storm in emergency dissemination. FT algorithm selects best disseminator by considering following metrics, forwarding probability, mobility, delivery delay and node degree.

(i) Forwarding Probability

Forwarding probability is described as the probability of forwarding received packet to the cluster member nodes.

Forwarding probability is computed as follows,

$$F_p = \alpha \cdot \frac{v}{v_{max}} + \frac{\beta}{R} \tag{37}$$

Where, α and β are weight factors, v denotes velocity of the vehicle and v_{max} denotes maximum velocity of the vehicle.

(ii) Delivery delay

Delivery delay is one of the significant metric to consider in best disseminator selection. Delivery delay metric is described as the time required to transmit the given packet to its neighbour. It can be expressed as follows,

$$D_d = \frac{P_L}{T} \tag{38}$$

Where, P_L denotes length of the packet and T represents the time required to transmit P_L. Mobility metric is defined as the moving behaviour of the vehicle with respect to the time which is computed using Equation (18). Node degree metric is computed using Equation (19).

These computed metric is given to the FT algorithm to select best disseminator. Herein, Fuzzy algorithm combined to calculate weight for each metrics. FT algorithm has following steps to rank the vehicles. FT algorithm

considers metrics as criteria's C_1-forwarding probability, C_2-Delivery delay, C_3-Mobility, C_{4-}node degree. The below matrix indicates cluster member criteria C_1- $C_{5,}$ These criteria values are known by the CH node.

Step 1:

In this step, values in the above table are not in the same range. Hence, we normalize the values using below equation,

$$N = \frac{x_{i,j} - \min_{\forall}(x_{i,j})}{\max x_{i,j} - \min_{\forall}(x_{i,j})} \tag{39}$$

Step 2:

In this step, weighted decision matrix is made by assigning criteria weights to each values of normalized matrix. Weighted normalized matrix W_k is expressed as follows,

$$W_k = \begin{bmatrix} X_{11} & X_{12} & X_{13} & X_{14} \\ X_{21} & X_{22} & X_{23} & X_{24} \\ \vdots & \vdots & \vdots & \vdots \\ X_{n1} & X_{n2} & X_{n3} & X_{n4} \end{bmatrix} \tag{40}$$

Step 3:

After completing normalization of decision matrix, each value is modified rendering to its rank. After that rank values are transformed to the fuzzy membership function which is explained in Table 5.

Step 4:

In this step, separation measures are computed via Euclidean distance of each value using Fuzzy Negative Ideal Solution (FNIS) and Fuzzy Positive Ideal Solution (FPIS).

Table 5 Fuzzy membership function

Rank	Membership Function
Very Low	0.00,0.05,0.15,0.19
Low	0.20,0.25,0.35,0.39
High	0.40,0.48,0.54,0.59
Very High	0.60,0.68,0.74,0.80

FPIS and FNIS are expressed as follows,

$$FPIS = (X_1^+, X_2^+, \ldots, X_n^+) = max_i\, X_{i,j}; \quad i = 1 \ldots m : \\ j = 1 \ldots n+1 \tag{41}$$

$$FPIS = (X_1^-, X_2^-, \ldots, X_n^-) = min_i\, X_{i,j}; \quad i = 1 \ldots m : \\ j = 1 \ldots n+1 \tag{42}$$

Step 5:

Final step in FT algorithm is rank index calculation where vehicle with highest rank is selected as best disseminator. Rank index is expressed as follows,

$$R_I = \frac{D^-}{D^+ + D^-} \tag{43}$$

Where,

$$D^+ = \sum_{i=1}^{4} \sqrt{\sum_{j=1}^{n+1} (X_{ij} - X_j^+)^2} \tag{44}$$

$$D^- = \sum_{i=1}^{4} \sqrt{\sum_{j=1}^{n+1} (X_{ij} - X_j^-)^2} \tag{45}$$

By means of using above Equation (42), we compute rank for vehicle according to its weight values. Vehicle which has highest rank is elected as best disseminator for each cluster. Selected disseminator functions fastly in disseminating emergency message to its cluster member that tends to reduce delay and broadcast storm.

5 Experimental Results

Experimental results section describes briefly about our DEMD^{2}RS work results and also compares result with existing method SSVC, CEMD, AEDS, SPMS and HMM. In this, DEMD^{2}RS and existing methods (mentioned above) are experimented in Omnet 4.6 and SUMO 0.21.0 simulators with 500 vehicular nodes, 2 RSU, 1 trusted authority and cloud server. The results obtained from this experimentation are discussed in comparative analysis section.

Here, we compared our DEMD^{2}RS work with the five existing methods. The reason behind choosing these methods is that contribution of these methods is similar to the contribution of this work. This section is further subdivided into three sections that are simulation setup, performance metrics and comparative analysis.

5.1 Simulation Setup

Our DEMD^{2}RS work is implemented in Omnet 4.6 and SUMO 0.21.0 simulation tool. Omnet is a Objective Modular Network Testbed is a modulator used to execute simulation like packet transmission and SUMO is a Simulation of Urban MObility which is traffic analyzer based network simulator. SUMO is used in road topology and traffic mobility pattern analysis. Omnet++ is an event based network simulator and SUMO is a road traffic simulator. Veins and Inet frameworks are also used in our simulation. In this, veins framework is used to integrate both SUMO (traffic) and Omnet++ (network) simulators and also simulates those in parallel. This is achieved through making Transmission Control Protocol (TCP) connection between SUMO and Omnet++ hence it could simulate both traffic and network. Inet is an open source model library of the Omnet++ simulation environment. Here, vehicles are generated in SUMO and then it is impart to the network simulator. Omnet++ considers all the vehicles as the nodes and simulates the scenario. If any changes occur in network environment, then veins change the vehicle scenario in the SUMO. Simulation parameter used in our DEMD^{2}RS work is detailed in Table 6. In our simulation environment, we consider number of accidents is 2. Besides, our network also performed well under high incidents scenario (such as more than 2 incidents) with the aid of our proposed FT based emergency dissemination mechanism. It selects the optimal disseminator quickly under high number of incidents using the benefits of both fuzzy and TOPSIS algorithms. Even for high incidents scenario, our method doesn't introduce broadcast storm and collisions due to selection of disseminator within the each cluster. Since our network is divided into the number of clusters initially.

Figure 4 illustrates the simulation environment of the proposed VANET-Cloud network. It comprises of the four entities that are vehicles, RSU, TA and cloud servers. This simulation environment represents the number of streets in the our proposed VANET-Cloud network. In addition, we don't consider any obstacles scenarios for VANET-Cloud network.

Table 6 Simulation parameters

Simulation Parameters			Values
Simulation Area			2500m×2500m
Number of Vehicle			500
Number of RSU			2
Number of Trusted Authority			1
Mobility type of the vehicle			TraCI mobility
Average Number of Vehicles (for each node)			5
Packet Traffic Type			Constant Bit Rate (CBR)
Communication Range of Vehicle			250m
Communication Interface			IEEE 802.11p
Encryption Parameters	Key size (bits)		192
	Block Size (bits)		128
	Number of round		16
Emergency Data (ED)	Number of accidents		2
	ED-1	Packet ID	435
		Event ID	1010
	ED-2	Packet ID	1955
		Event ID	1307
Vehicle speed			0–50m/s
Simulation time			500s

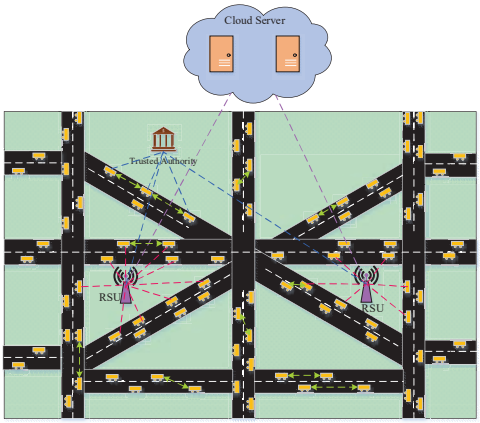

Figure 4 Simulation environment.

5.2 Performance Metrics

Our DEMD^{2}RS work performances are evaluated using consequent metrics for instance Throughput, Packet Delivery Ratio, Transmission delay, Average

delay, Key generation time, Encryption time and Decryption time. These metrics are signified as follows,

(A) Throughput

Throughput metric is described as the maximum rate at which the packets are delivered over the network. Through metric is evaluated in order to measure efficiency of data transmission. It can be expressed as follows:

$$\textit{Throughput} = \frac{N_P}{\mathcal{T}} \tag{46}$$

Where, N_P represents the number of packets transmitted over time $\mathcal{T}$.

(B) Packet Delivery Ratio

Packet delivery ratio is the ratio of data packets received at the destination $(P_{r,\mathbb{D}})$ with respect to the number of packets transmitted from the source $(P_{t,s})$. This metric is used to evaluate the efficiency and correctness of the routing performed in VANET-Cloud environment. It can be measured as follows:

$$PDR = \frac{P_{r,\mathbb{D}}}{P_{t,s}} \tag{47}$$

(C) Average delay

Average delay metric is used to measure the ordinary delay in data transmission. It is described as average of how much time taken to transmit given packet to the destination. This metric is obtained using below expression:

$$A_d = \frac{\sum_{i=0}^{n} t_i/n}{\sum_{i=0}^{l} P_i/l} \tag{48}$$

Where, $\sum_{i=0}^{n} t_i$ represents the average time and $\sum_{i=0}^{l} P_i/l$ represents the average number of packets.

(D) Transmission Delay

Transmission delay metric is defined as the time required by the packet to receive its destination. This metric can be used to measure the correctness of the DEMD^{2}RS system in terms of delay in transmission. This metric is acquired using below expression:

$$\mathbb{T}_d = \frac{P_s}{T_r} \tag{49}$$

Where, P_s indicates the size of the packet and T_r indicates the transmission rate.

(E) Key Generation Time

Key generation metric is used to evaluate the proficiency of the DEMD^{2}RS encryption algorithm. It is the time required to generate keys for encryption process. It is estimated using the below expression:

$$K_g = \frac{N_k}{\mathcal{T}} \tag{50}$$

Where N_k indicates the number of key generated over time $\mathcal{T}$.

(F) Encryption Time

Encryption time is referred as the time taken to complete encryption for given data. It is used to measure the computation speed of the DEMD^{2}RS encryption algorithm.

$$E_{\mathcal{T}} = \frac{P_e}{\mathcal{T}} \tag{51}$$

Where P_e represents the packet encrypted over time $\mathcal{T}$.

(G) Decryption Time

Decryption time is described as the time required to complete decryption of given plain data. This metric is used to evaluate the decryption performance of the proposed algorithm.

$$D_{\mathcal{T}} = \frac{P_d}{\mathcal{T}} \tag{52}$$

Where, P_d represents the packet decrypted over time $\mathcal{T}$.

5.3 Comparative Analysis

Comparative analysis section elaborates comparison of DEMD^{2}RS work results with the existing SSVC, CEMD, AEDS, HMM and SPMS. We compare DEMD^{2}RS work performance using aforementioned methods with the succeeding performance metrics.

5.3.1 Analysis on throughput

Throughput metric is significant to evaluate in regard to discover performance of the DEMD^{2}RS work. We measure throughput performance with respect

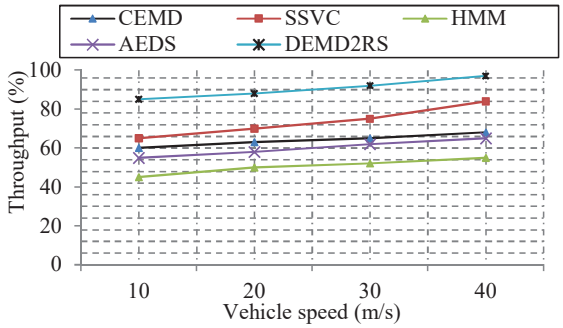

Figure 5 Comparisons on throughput.

to the vehicle speed. Throughput metric is as much as possible to improve performance of the DEMD^{2}RS work.

Figure 5 illustrates the comparison on throughput that shows our DEMD^{2}RS method achieves better throughput compared to the existing SSVC, CEMD, HMM and AEDS. Our DEMD^{2}RS method achieves maximum of 97% as throughput. Since, we propose ANN based routing that selects vehicle with highest weight to transmit information to the destination vehicle. ANN also preserves security in data transmission. This way of sending packets to the destination vehicle reduces packet loss that tends to increase the throughput of the DEMD^{2}RS work. In mean time, existing SSVC, CEMD, HMM and AEDS methods doesn't performed effective routing to transmit data packet to the destination vehicle. It tends to more packet loss during data packet transmission that reduces the throughput. Since, data packet transmission doesn't perform any unique path identification mechanism. From this analysis, we conclude that, DEMD^{2}RS method achieves better throughput performance compared to the existing methods.

5.3.2 Analysis on transmission delay

Transmission delay metric is evaluated to measure the delay in emergency message dissemination. This metric defines efficacy of the DEMD^{2}RS delay aware emergency dissemination. We measure transmission delay in milli seconds (ms) with respect to number of vehicles. Here, we compare DEMD^{2}RS work with the three existing methods that are CEMD, AEDS and SSVC. This is due to the fact that, these methods are contributes emergency dissemination in vehicular cloud network.

Figure 6 demonstrates comparison of transmission delay with respect to the number of vehicles that concludes our DEMD^{2}RS method achieves

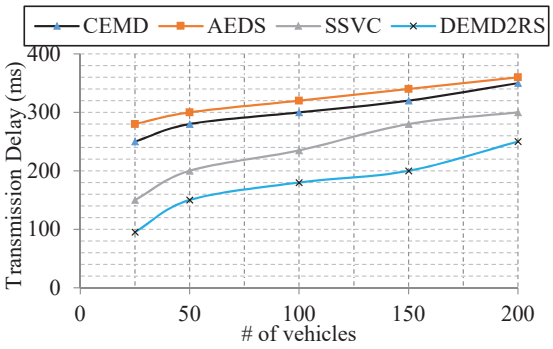

Figure 6 Comparisons on Transmission delay vs. number of vehicles.

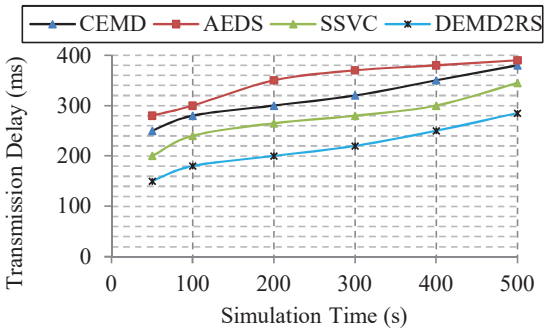

Figure 7 Comparisons on Transmission delay vs. Simulation time.

less transmission delay for 200 vehicles. Since, our DEMD^{2}RS work forms stable cluster using FACS method. Herein, if any accident occurs within the cluster, CH selects best disseminator through FT algorithm. FT algorithm considers four metrics that are related to reduce delay in emergency message dissemination such as forwarding probability, delivery delay, mobility and node degree. These metrics are significant to reduce delay. In addition to it, it also reduce broadcast storm in emergency message dissemination, since disseminator vehicle only disseminates emergency information to its cluster member. Hence, our method achieves minimum transmission delay of 65ms for 200 vehicles whereas existing methods has more delay as maximum of 345ms for 200 vehicles.

Figure 7 illustrates the comparisons on transmission delay with respect to the simulation time that determines DEMD^{2}RS method has less transmission delay compared to the existing SVCC, CEMD and AEDS. DEMD^{2}RS method achieves minimum of 180 ms for 500 s. The existing method such

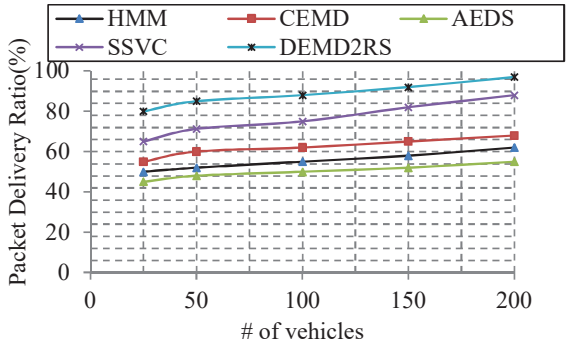

Figure 8 Comparisons on Packet delivery Ratio vs. number of vehicles.

as SVCC, CEMD, and AEDS doesn't considered effective method to route the packets to the destination node that tends to increase in the transmission delay. From the above comparison results define AEDS has maximum transmission delay. Herein, AEDS doesn't consider metrics such expected transmission time, expected transmission count, distance metrics to route the packets to the destination. These leads to increase in transmission delay of AEDS method. Hence, it has maximum of 350secs for simulation time of 500secs. From the comparison of transmission delay with respect to both simulation time and number of vehicles defines DEMD^{2}RS method achieves better results in transmission delay.

5.3.3 Analysis on packet delivery ratio

Packet delivery ratio metric is one of the significant metric to evaluate performance of the DEMD^{2}RS work. Packet Delivery Ratio metric is high as much as possible, in order to increase the performance of DEMD^{2}RS work. We measure packet delivery ratio in percentage with respect to the number of vehicles.

Figure 8 depicts the comparison on packet delivery ratio results with respect to the existing methods including SSVC, CEMD, AEDS and HMM. The comparison results bring about DEMD^{2}RS method has high packet delivery ratio compared to the SSVC. Since, DEMD^{2}RS method runs ANN algorithm to determine weights for each vehicular nodes. ANN has many advantages in terms of solution finding. ANN works fast compared to the other algorithm that leads to reduce time needed to select optimum vehicles. Highest weighted vehicles are selected to transmit data packets to the destination. This way of routing increases packet delivery ratio of the DEMD^{2}RS work. Hence, DEMD^{2}RS method achieves maximum packet delivery ratio of

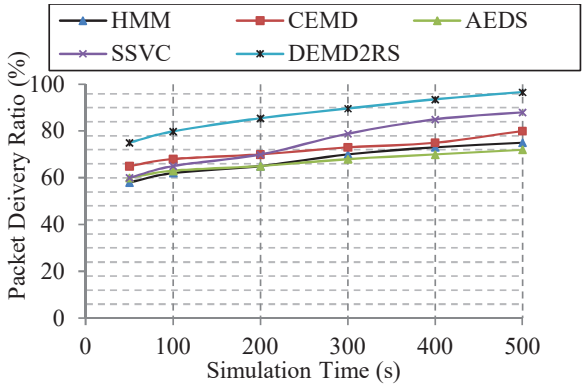

Figure 9 Comparisons on Packet delivery Ratio vs. Simulation time.

97% for 200 vehicles compared to existing methods. From this comparison, we prove that our method achieves better packet delivery ratio in both very small and very high density of vehicles. Since our method achieves maximum of 80% in packet delivery ratio for 50 vehicles and maximum of 99% for packet delivery ratio for 200 vehicles. Therefore, we conclude that our method achieves better performance for both very small and very high cases.

Figure 9 shows the comparison on packet delivery ratio with respect to the simulation of time 500secs. From the above simulation results, we conclude that our DEMD^{2}RS method achieves reduce packet loss compared to the existing SSVC, CEMD, AEDS and HMM. Since, existing methods achieves doesn't perform optimum path selection while transmitting data packet to the destination that leads to reduce packet delivery ratio. From the comparison of packet delivery ratio with respect to the simulation time and number of vehicles, we conclude that DEMD^{2}RS method achieves better performance in packet delivery ratio.

5.3.4 Analysis on average delay

Average delay metric is important to consider in proposed DEMD^{2}RS work. Since, it regulates the performance of the DEMD^{2}RS in terms of the data transmission. Average delay metric is measured in ms with respect to the number of vehicles.

Figure 10 depicts the comparison on average delay results with respect to the existing methods SSVC, CEMD, AEDS and HMM. Since, ANN based routing method considers six metrics to route the packet to the destination. Herein, expected transmission time and expected transmission count metrics

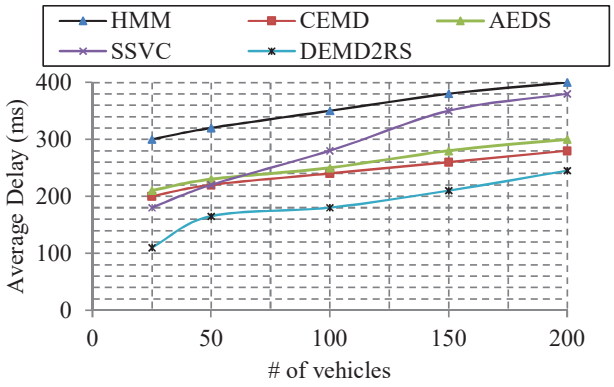

Figure 10 Comparisons on average delay.

Table 7 Comparison of DEMD^{2}RS and existing methods on network efficiency

Metrics		HMM	CBED	AEDS	SSVC	DEMD^{2}RS
Throughput (%)		50.5	64	60	74	**91**
Transmission	# of vehicle	–	300	320	272	**213**
Delay (ms)	Simulation time	–	313	345	295	**272**
Packet delivery	# of vehicle	55.4	62	50	76	**88**
Ratio (%)	Simulation time	67.1	71	66	77	**89**
Average Delay (ms)		350	240	254	282	**182**

plays vital role to transmit data packets to the destination. These metrics reduces transmission delay and also reduces loss in data transmission effectually. Hence, our method achieves less average delay as 240 ms for 200 vehicles.

Table 7 illustrates the comparison of proposed and existing methods on network efficiency. From which, we conclude DEMD^{2}RS method performs better than existing methods.

5.3.5 Analysis on key generation time

Key generation time is most important in secure integration of cloud and VANET. Since, this metric defines performance of DEMD^{2}RS security methods.

Figure 11 provides comparisons on key generation time of DEMD^{2}RS and existing SSVC and SPMS method. In this, we have compared DEMD^{2}RS work with two methods that are SPMS and SSVC. Since, these two methods only concentrated on the securing cloud data and providing authentication to

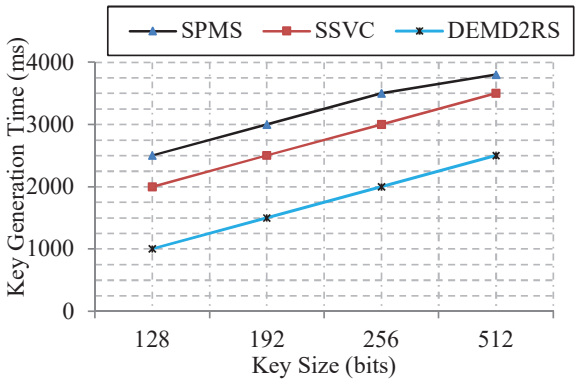

Figure 11 Comparisons on key generation time.

the vehicular nodes. Result of this comparison shows DEMD^{2}RS Twofish algorithm has less key generation time compared to the existing blowfish algorithm based encryption in SSVC and SPMS. Our Twofish algorithm performs fastly in key generation that tends to achieve minimum key generation time as 2500 ms for 512 bits key. Whereas existing blowfish encryption has maximum of 3500 ms for 512 bit key sizes. Blowfish runs slowly compared to Twofish that leads to the increase in key generation time.

5.3.6 Analysis on encryption time

Encryption time metric is used to evaluate the time needed to encrypt the given plain data in our DEMD^{2R}S method. This metric provides efficiency of DEMD^{2}RS encryption method. Herein, we measure encryption time using data packet size. In this comparison, we compared DEMD^{2}RS work with the two existing methods that are SPMS and SSVC. Since, these two methods only considered the security of the cloud data and provides authentication to the vehicular nodes.

Figure 12 illustrates comparisons on encryption time of DEMD^{2}RS and existing methods. DEMD^{2}RS twofish algorithm has maximum encryption time of 4990ms for 50MB of data packet. Since, twofish algorithm has 16 rounds to encrypt plain data whereas other symmetric key encryption algorithm has more rounds to generates encrypted data that leads to reduce encryption time. In the mean time, blowfish algorithm has block size 64 bits which is less compared to the twofish algorithm that leads to increase encryption time. Hence, DEMD^{2}RS method achieves minimum encryption time as 4800ms for 50MB of data packet size.

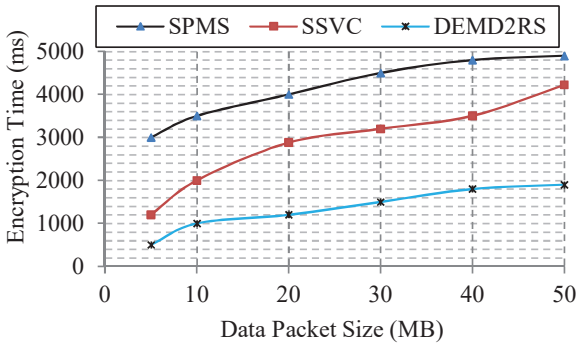

Figure 12 Comparisons on encryption time.

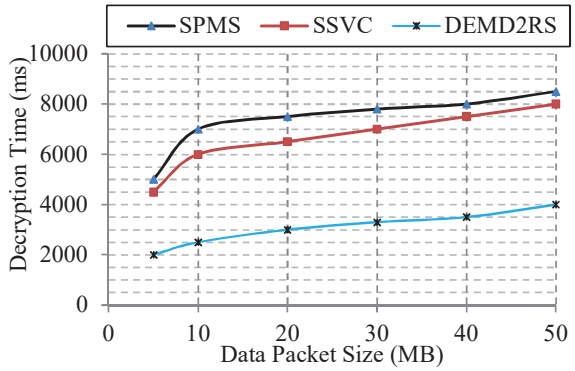

Figure 13 Comparisons on decryption time.

5.3.7 Analysis on decryption time

Decryption time metric is used to evaluate the performance of the DEMD^{2}RS decryption. Evaluation of decryption provides proficiency of DEMD^{2}RS security scheme. In this, we have compared DEMD^{2}RS work with two methods that are SPMS and SSVC. Since, these two methods only concentrated on the securing cloud data and providing authentication to the vehicular nodes.

Figure 13 designates comparisons on decryption time of DEMD2RS and existing works. The above comparison results shows DEMD2RS method achieves less decryption time compared to the existing SVCC and SPMS method. Our DEMD^{2}RS twofish algorithm performs better than blowfish algortihm in terms of decryption. Twofish algorithm performs fast that leads to reduce time required to key generation and encryption. In symmetric encryption algorithm, decryption is reverse process of encryption that tends to

Table 8 Comparison of DEMD^{2}RS and existing methods on security efficiency

Metrics	SPMS	SSVC	DEMD^{2}RS
Key Generation Time (ms)	3200	2750	**3750**
Encryption Time (ms)	4116	3834	**3250**
Decryption Time (ms)	7300	7600	**3050**

reduce time required to compelete conversion of cipher text to the plain text. Hence, our DEMD^{2}RS method has minimum decryption time as 7885 ms for 50 MB of data packet size. Meanwhile, existing blowfish algorithm requires more time for key generation and encryption that tends to increase the decryption time. Hence, decryption time of existing method is maximum as 9500ms for 50MB data packet size.

Table 8 explains about average values of evaluation metrics comparisons where DEMD^{2}RS, SPMS and SSVC methods are compared. The reason for selecting SPMS and SSVC methods for security efficiency comparison is that, these methods only provides security in VANET integrated Cloud network. From which, we confirm that our DEMD^{2}RS method achieves better performance in secure VANET-Cloud environment.

5.4 Communication Cost

The communication cost of the proposed work is estimated with the aid of the number of messages transmitted and time required to transmit the message.

Assume that, our network has 100 messages for transmission. Here, 70 messages are the normal messages to transmit between source and destination. And, the 30 are related to the safety dissemination. For normal transmission between source and destination, our method uses the ANN based routing which estimates path quickly with reduced time as 240 ms compared to the existing mechanism. Likewise, emergency message dissemination is performed through FT algorithm which selects the optimal with less time as 340 ms compared to the existing mechanism. From this evaluation, we conclude that our proposed DEMD^{2}RS has less communication cost.

5.5 Security Analysis

This section deliberates security analysis of our work with respect to the number of of attacks introduced by the malicious users. In our proposed work, we have assumed malicious nodes in the network is below 25% of the overall density. Hence, our VANET-Cloud network is not fully comporomised by

the malicious node. Under this situation, our proposed method effectively mitigate the attacks in the VANET-Cloud network. Our main intent is to mitigate succeeding attack such as password spoofing attack, Man-In-Middle attack and Sybil attack.

5.5.1 Password spoofing attack

Password spoofing attack is very dangerous attack where malicious users steal password from legitimate users. Using this passowrd, malicious users gets information from cloud and use it in illegal manner. This attack is mitigated via our proposed HCAS where Secure Hash Algorithm-3 (SHA-3) and Elliptic Curve Points (ECP) algorithms are used to provide high security to the users credentials. Out TA provides passwords to each user which comprises of concatenation of hash values of three unique parameters of each vehicle that are L.No, P.No and C.No. In this we take last four digits from C.No since it contains twelve digits. Hash values of three credentials are estimated via SHA-3 algorithm which is highly secure algorithm. Psuedo ID is generated from ECP which is unique for each vehicle. This way of generating password provides more security to the VANET-Cloud network. Hence, malicious users cannot spoof legitimate users information.

5.5.2 Man-In-The-Middle attack

Man-In-The-Middle attack is one of hazardous attack where attackers eavesdrop to the communication channels between Cloud and RSU, RSU and Vehicle. In order to overwhelm this attack, we encrypt data using Twofish algorithm. Twofish algoirthm provides high security to the transmitted information from cloud to RSU. Twofish is a symmetric key cryptography algorithm which has 128 bit symmetric block size and key length as 128, 192 and 256 bits with 16 rounds. Twofish doesn't generate weak key which provides high security to the data. After receving data, encrypted information is transmitted via secure routing which is executed in RSU via implementing ANN algorithm. Thus results in highly secure communication between Cloud, RSU and Vehicles.

5.5.3 Sybil attack

The sybil attack is the one of the severe attacks in the vehicular environment. In sybil attack, the malicious users forges multiple identities and use these identities to interrupt the functionality of the VANET network by disseminating false identities. In our network, we mitigate this attack via highly secure authentication process. Here, the credentials of the user is secured via the

SHA-3 and ECP algorithms. Using SHA-3 algorithm user find hash value for their credentials. These values are provided to the TA which generates pseudo ID and password using the recevied hash based credentials. Here, the pseduo ID is generated with the aid of the ECP. Hence, the credentials of the user is cannot be forged by the malicious users. Therefore, our VANET-Cloud network is secured against the sybil attack.

6 Conclusion

To date, VANET integrated Cloud technology evolving day by day due to the huge mass of vehicles. This paper proposes a secure cloud integrated VANET. Contributions of this work are divided into four fold that are authentication, Clustering, Data retrieval and Data dissemination. Authentication is performed through the HCAS method, in order to avoid malicious users forging behaviors. Clustering is executed using FACS where SKH algorithm is proposed that preserves constant behaviour of the cluster. Data retrieval process, user requested informations are provided after completion of credentials verification. Cloud sends encrypted data to the request vehicle via RSU. RSU executes ANN algorithm to deliver received information. Data dissemination process is executed using FT algorithm which is handled by the CH vehicle. Best disseminator is selected using FT algorithm and then emergency data are disseminated to the cluster member without any delay. Finally, we evaluate performance of the DEMD^{2}RS work using following metrics Throughput, Transmission delay, Average delay, Key generation time, Encryption time and decryption time. From the comparison results, we show that DEMD^{2}RS method achieves better performance compared to the existing SSVC method.

6.1 Future Work

In future, we intend to propose attack (Spamming and DDos attack) detection in VANET-Cloud environment. In addition to it, we also verify integrity of the retrieved data. We will test our DEMD^{2}RS delay aware emergency dissemination in application scenario.

References

[1] Rasheed Hussain, Zeinab Rezaeifar, Junggab Son, Md Zakirul Alam Bhuiyan, Sangjin Kim, Heekuck Oh, “PB-MII: replacing static RSUs

with public buses-based mobile intermediary infrastructure in urban VANET-based clouds", Cluster Computing, Volume 20, Issue 3, pp. 2231–2252, 2017

[2] Rakesh Shrestha, Rojeena Bajracharya, and Seung Yeob Nam, "Challenges of Future VANET and Cloud-Based Approaches", Wireless Communications and Mobile Computing, Volume 2018, pp. 1–15, 2018

[3] Qamas Gul Khan Safi, Senlin Luo, Chao Wei, Limin Pan Guanglu Yan, "Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs", Computer Standards & Interfaces, Volume 56, pp. 107–115, 2018

[4] Qamas Gul Khan Safi, Senlin Luo, Limin Pan,Wangtong Liu, Guangluo Yan, "Secure authentication framework for cloud-based toll payment message dissemination over ubiquitous VANETs", Pervasive and Mobile Computing, Volume 48, Pages 43–58, 2018

[5] Qamas Gul Khan Safi, Senlin Luo, Chao Wei, Limin Pan Qianrou Chen "PIaaS: Cloud-oriented secure and privacy-conscious parking information as a service using VANETs", Computer Networks, Volume 124, pp. 33–45, 2017

[6] Raghavendra Pala, Arun Prakasha, Rajeev Tripathia, Dhananjay Singhb, "Analytical model for clustered vehicular ad hoc network analysis", ICT Express, Volume 4, pp. 160–164, 2018

[7] Xiang Ji, Huiqun Yu, Guisheng Fan, Huaiying Sun, and Liqiong Chen, "Efficient and Reliable Cluster-Based Data Transmission for Vehicular Ad Hoc Networks", Mobile Information Systems, Volume 2018, pp. 1–15, 2018

[8] Islam Tharwat Abdel-Halim, Hossam Mahmoud Ahmed Fahmy, Ayman M. Bahaa-ElDin, "Mobility Prediction-based Efficient Clustering Scheme for Connected and Automated Vehicles in VANETs", Computer Networks, Volume 150, Pages 217–233, 2019

[9] Rejab Hajlaoui, Eesa Alsolami, Tarek Moulahi, Hervé Guyennet, "Construction of a stable vehicular ad hoc network based on hybrid genetic algorithm", Telecommunication Systems, pp. 1–13, 2018

[10] Chao Song, Jie Wu, Ming Liu, Huanyang Zheng, "Efficient routing through discretization of overlapped road segments in VANETs", Journal of Parallel Distributed Computing, Volume 102, Pages 57–70, 2017

[11] Junling Shi, Xingwei Wang, Min Huang, Keqin Li, Sajal K. Das, "Social-based routing scheme for fixed-line VANET", Computer Networks, Volume 113, pp. 230–243, 2017

[12] Osama Rehman, Mohamed Ould-Khaoua, "A hybrid relay node selection scheme for message dissemination in VANETs", Future Generation Computer Systems, Volume 93, Pages 1–17, 2019
[13] Renöe Oliveira, Carlos Montez, Azzedine Boukerche, Michelle S. Wangha, "Reliable Data Dissemination Protocol for VANET Traffic Safety Applications", Ad Hoc Networks, Volume 63, Pages 30–44, 2017
[14] Truc D.T. Nguyen, Thanh-Van Le, Hoang-Anh Pham, "Novel store–carry–forward scheme for message dissemination in vehicular ad-hoc networks", ICT Express 3, 193–198, 2017
[15] Syed Sarmad Shah, Asad Waqar Malik, Anis U. Rahman Sohail Iqbal, and Samee U. Khan, "Time Barrier-Based Emergency Message Dissemination in Vehicular Ad-hoc Networks", IEEE Access, Volume 7, pp. 16494–16503, 2019
[16] Odongo Steven Eyobu, Jhihoon Joo, and Dong Seog Han, "CMD: A Multichannel Coordination Scheme for Emergency Message Dissemination in IEEE 1609.4", Mobile Information Systems, Volume 2018, pp. 1–13, 2018
[17] Kai Fan, Xin Wang, Katsuya Suto, Hui Li, and Yintang Yang, "Secure and Efficient Privacy-Preserving Ciphertext Retrieval in Connected Vehicular Cloud Computing", Volume: 32, Issue: 3, pp. 52–57, 2018.
[18] Yixian Yang, Xinxin Niu, Lixiang Li, and Haipeng Peng, "A Secure and Efficient Transmission Method in Connected Vehicular Cloud Computing", Volume: 32, Issue: 3, pp. 14–19, 2018
[19] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, Anis Laouiti, "Trust model for secure group leader-based communications in VANET", Wireless Networks, pp. 1–23, 2018
[20] Abderrahim Abdellaoui, Oussama Azzam, Habiba Chaoui, Hicham elachgar, Nabil Hmina, "xxTEA-VCLOUD:A Security Scheme for the Vehicular Cloud Network using a Lightweight Encryption Algorithm", CCIOT 2018 Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things, pp. 67–72, 2018
[21] Lei Liua, Chen Chena, Tie Qiub, Mengyuan Zhanga, Iyu Lia, Bin Zhouc, "A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs", Vehicular Communications, Volume 13, pp. 78–88, 2018
[22] Sarah Oubabas, Rachida Aoudjit, Joel J.P.C. Rodrigues, Said Talbi "Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme", Vehicular Communications, Volume 13, Pages 128–138, 2018

[23] Yasir Ali Shah, Hafiz Adnan Habib, Farhan Aadil, Muhammad Fahad Khan, Muazzam Maqsood, and Tabassam Nawaz, "CAMONET: Moth-Flame Optimization (MFO) Based Clustering Algorithm for VANETs", IEEE Acces, Volume: 6, pp. 48611–48624, 2018

[24] Yassine Hernafi, Mohamed Ben Ahmed, Mohammed Bouhorma, "ACO and PSO Algorithms for Developing a New Communication Model for VANET Applications in Smart Cities", Wireless Personal Communications, Volume 96, Issue 2, pp. 2039–2075, 2017

[25] Hui Xi, San-shun Zhang, Ben-xia Li, Li Li, and Xiang-guo Cheng, "Towards a Novel Trust-Based Multicast Routing for VANETs",, Security and Communication Networks, Volume 2018, p. 12, 2018

[26] Sha Wang, Chuanhe Huang, Danxin Wang, "Delay-aware relay selection with heterogeneous communication range in VANETs", Wireless Networks, pp. 1–10, 2018

[27] Li, T., Xiong, N. N., Gao, J., Song, H., Liu, A., and Cai, Z., "Reliable Code Disseminations through Opportunistic Communication in Vehicular Wireless Networks", IEEE Access, 2018

[28] [Daxin Tian, Chao Liu, Xuting Duan, Zhengguo Sheng, Qiang Ni, Min Chen, and Victor C.M. Leung, "A Distributed Position-Ba IEEE Internet of Things Journal, Volume: 5, Issue: 2, pp. 1218–1227, 2018

[29] Yusor Rafid Bahar Al-Mayouf, Omar Adil Mahdi, Namar A. Taha, Nor Fadzilah Abdullah, Suleman Khan, and Muhammad Alam, "Accident Management System Based on Vehicular Network for an Intelligent Transportation System in Urban Environments", Journal of Advanced Transportation, Volume 2018, 11 pages, 2018

[30] Wei-Chen Wu, "A secret push messaging service in VANET clouds", The Journal of Supercomputing, Volume 73, Issue 7, pp. 3085–3097, 2017

[31] SathyaNarayananP.S.V, "A sensor enabled secure vehicular communication for emergency message dissemination using cloud services", Digital Signal Processing, Volume 85, Pages 10–16, 2019

[32] B. Ramakrishnan, R. Bhagavath Nishanth, M. Milton Joe, M. Selvi, "Cluster based emergency message broadcasting technique for vehicular ad hoc network", Wireless Networks, Volume 23, Issue 1, pp. 233–248, 2017

[33] Lin Yao, Jie Wang, Xin Wang, Ailun Chen, and Yuqi Wang, "V2X Routing in a VANET Based on the Hidden Markov Model", IEEE Transactions On Intelligent Transportation Systems, Volume: 19, Issue: 3, pp. 889–899, 2018

[34] Jian Shen, Chen Wang, Aniello Castiglione, Dengzhi Liu and Christian Esposito, "Trustworthiness Evaluation-based Routing Protocol for Incompletely Predictable Vehicular Ad hoc Networks", IEEE Transaction on Big data, 2017

[35] Yao-Hsin Chou, Ting-Hui Chu, Shu-Yu Kuo, and Chi-Yuan Chen, "An Adaptive Emergency Broadcast Strategy for Vehicular Ad hoc Networks", IEEE Sensors Journal, Volume: 18, Issue: 12, pp. 4814–4821, 2018

[36] Lap-piu Lee and Kwok-wo Wong, "An elliptic curve random number generator", Communications and Multimedia Security Issues of the New Century, pp. 127–133, 2010

[37] Wang, G.-G., Gandomi, A. H., and Alavi, A. H. "Stud krill herd algorithm", Neurocomputing, Volume 128, pp. 363–370, 2014

[38] Heba Harahsheh, Mohammad Qatawneh, "Performance Evaluation of Twofish Algorithm on IMAN Supercomputer", International Journal of Computer Applications (0975–8887), Volume 179, Issue 50, 2018

Biography

M. Al-Shabi received his bachelor's degree (B.Sc. Computer Science) from Technology University at Iraq (1997), Postgraduate Master (M. Sc. Computer Science from Putra Malaysia University at 2002), and Ph.D. (Computer Science) from Putra Malaysia University, Malaysia (2006). He is currently an associate professor in the Department of Management Information System, College of Business Administration at Taibah University, Kingdom of Saudi Arabia. Prior to joining Taibah University, he worked in the faculty of a computer at Qassim University, Saudi Arabia. His research interests include wireless security, cryptography, UML, Stenography Multistage interconnection network, Vehicular Ad-hoc Network-Cloud, Smart and Intelligent computing and Apply Mathematically.