Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.026152
Article

Intelligent Vehicular Communication Using Vulnerability Scoring Based Routing Protocol

M. Ramya Devi* and I. Jasmine Selvakumari Jeya

Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, 641050, India
*Corresponding Author: M. Ramya Devi. Email: ramyamurugadasan@gmail.com
Received: 16 December 2021; Accepted: 16 February 2022

Abstract: Internet of Vehicles (IoV) is an intelligent vehicular technology that allows vehicles to communicate with each other via internet. Communications and the Internet of Things (IoT) enable cutting-edge technologies including such self-driving cars. In the existing systems, there is a maximum communication delay while transmitting the messages. The proposed system uses hybrid Cooperative, Vehicular Communication Management Framework called CAMINO (CA). Further it uses, energy efficient fast message routing protocol with Common Vulnerability Scoring System (CVSS) methodology for improving the communication delay, throughput. It improves security while transmitting the messages through networks. In this research, we present a unique intelligent vehicular infrastructure communication management framework. This framework includes additional stability for both short and long-range mobile communications. It also includes built-in cooperative intelligent transport system (C-ITS) capabilities for experimental verification in real-world contexts. In addition, an energy efficient-fast message distribution routing protocol (EE-FMDRP) has been presented. This combines the benefits between both temporal and direction oriented routing methods. This has been suggested for distributing information from the origin ends to the predetermined objective in a quick, accurate, and effective manner in the event of an emergency. The critical value scale score (CVSS) employ ratings to measure the assault probability in Markov chains. Probabilities of chained transitions allow us to statistically evaluate the integrity of a group of IoV assets. Thus the proposed method helps to enhance the vehicular systems. The CAMINO with energy efficient fast protocol using CVSS (CA-EEFP-CVSS) method outperforms in terms of shortest transmission latency achieves 2.6 sec, highest throughput 11.6%, and lowest energy usage 17% and PDR 95.78%.

Keywords: Intelligent automation; intelligent transport system; vehicular networks; markov chains; internet of vehicles; critical value scale score

1 Introduction

An automobile having self-driving capabilities was increasingly common upon the roadways in recent decades. Massive technology and development attempts are taken to contribute in helping information to vehicles in time. Technology enables sharing of information among them and their environment, also renowned as Vehicle-to-everything (V2X) communication systems. It helps in sequence to increase safe driving and then further force the above protest movement [1]. Several modern communications systems were created in the past decade to offer direct data transfer in allocated frequency. They are centered on 802.11p and comprises of various Intelligent Transport Systems (ITS) layered architecture in Europe and the United States. Especially ITS-G5 and Dedicated Short Range Communication (DSRC) [2] are widely used. Similarly, increased connection leads to increased complication that creates wider system vulnerabilities from the security point of view. Intruders that developing the capacity IoV network weaknesses will have great possibilities to control automobiles. As a result, the risk of cyber-attacks that compromise secure operation, whether by mistake or on intent rises [3]. The subject on traffic during of messaging broadcast has been studied, and a mitigating mechanism named triple developing system has indeed been devised. Even as title implied, the strategy included a reinforcement system, a length system, and a place arrangement. Theories, on the other hand, are perfectly suited to the Vehicular environments, with no regard for the VANET's complex nature [4].

The Authorizing act aims to establish specifications for C-ITS units and operations, supporting the ITS-G5 specification as the industry norm for straight vehicle-to-infrastructure connection. The 5855–5925 MHz ITS range, on either hand, should remain technologically neutrality, according to European spectrum laws. That means whether any handheld radios that could also is such with Handheld Radios Directive's fundamental standards (for example, by complying with EN 302 571 may function in the ITS spectrum [5].

Many car and truck companies are currently hesitant to choose and incorporate a single technology. They are closely following development both in fields inx order to determine which one will eventually overtake inside the near. Several Original Equipment Manufacturers (OEM), from the other hand, already have begun to integrate short - read V2X technologies. For instance, Volkswagen, was one Europe's most popular automakers, had announced recently Golf 8 using its Car2X technologies [6].

The proposed CA-EEFP-CVSS method helps to improve the communication delay, throughput and gives security while transmitting the messages through networks. The research helps to identify the solutions for:

- How the Energy Efficient routing protocol sends the message in the faster way?
- How the CVSS using markov chains?
- How the security is given during the message transmission?

The major contribution of the proposed system is given below:

1. A automobile there at sender side transmits to identify demand to the neighbour set [Ns(Vx)], which lists the restricted broadcasting terminals are within the defined network area.
2. The automobile path permission or denial by the bi-directional modeling approach of passing traffic improves the EE-FMDRP. Unnecessary information transmission is reduced as a result of this, lowering network cost and saving power.
3. This method chooses the best gateways (passing partners) for message transmission with the shortest information transmission time possible.
4. The appropriate inter-mediate is chosen to define the fastest way.

The rest of our research article is written as follows: The Section 2 consists of brief study of existing Co-operative, Vehicular Communication Management Framework (CAMINO), energy efficient-fast message distribution routing protocol (EE-FMDRP) and Energy Efficient fast message routing protocol with Common Vulnerability Scoring System (CVSS). Section 3 describes the working principal of the proposed model. Section 4 evaluates the result and gives a comparison of different algorithms. Section 5 concludes the research work.

2 Related Work

In [7], the researchers provide a summary of hybrids Message integrity, define their possibilities, highlight obstacles, and explore significant design considerations. According to them, neither of today's political V2X solutions can meet the different Quality of Service (QoS) demands of linked vehicle scenarios [8–12]. Multi-Radio Access Technology (RAT) coordinating using hybrids V2X communication may be able to efficiently deal with different situations of a vehicle environment that meets QoS standards by picking the finest techniques. The writers discuss various communications patterns that include the RAT, its operating style (for example, lengthy or immediate), as well as other unique variables. Several patterns could be combined to boost capacity or utilized simultaneously to improve link dependability.

In [13], the author has supplied an updated copy of the slotting 1-persistence technique, as well as a method termed reliable and inexpensive broadcast Simple Robust Dissemination (SRD). The improved section describes priorities on roadways both for traffic orientations. A new mechanism dubbed safety messages distribution for automobiles (EMDV) was introduced [14]. To use a moving zone and a congestion mechanism, the method improved message transmission reliability. In [15] the author analyzed two-dimensional metropolitan situations and created the urban multi-hop broadcasting protocols (UMB) to address the problems of broadcast storm, and behind, and quality of service.

Improved information distribution dependent on guidance documents (eMDR) was produced in a study [16] that employed a map viewer and GPS to identify the location of the vehicle. In addition, [17] proposed an improved model of DV- CAST called urban vehicle broadcasting (UV-CAST), wherein the waiting period for re-dissemination of information is calculated based on distance among cars and site. Just at number of joints where signals are intended to be disseminated to multi-directional locations, the least latency performance is obtained. The DRIVE-data distribution strategy in vehicular networks discussed aggregating neighbor list into different groups for effective transmission process across both city driving scenarios [18–22].

3 Proposed Methodology

The proposed CA-EEFP-CVSS method is a flexible platform for V2X connectivity; it integrates common vulnerability scoring system to enhance the security while transmitting the messages over the networks and also provides many services. EE-FMDRP gives more proficient route among the starting place and end. It helps to reduce the delay and it improves the throughput of the system. Fig. 1 shows the overall architecture of CA-EEFP-CVSS.

3.1 Camino

CAMINO supports C-ITS operations in a dynamic, enabled the firm and supports mixed connectivity by interacting with such a range of social media components. The CAMINO-Core factor responsible the main functions needed to govern information flows here between northern and southern ports. CAMINO-Core links to various V2X telecommunications systems utilizing distinct transmitter subclasses at the data link. This can, for instance, connect using commercialized C-V2X PC5 and ITS-G5 units over UDP

connections with such a unique preamble, with a Message broker over TCP via cable or cell phones. Its Communications Control enables the transmitter types to communicate only with CAMINO-Core functions.

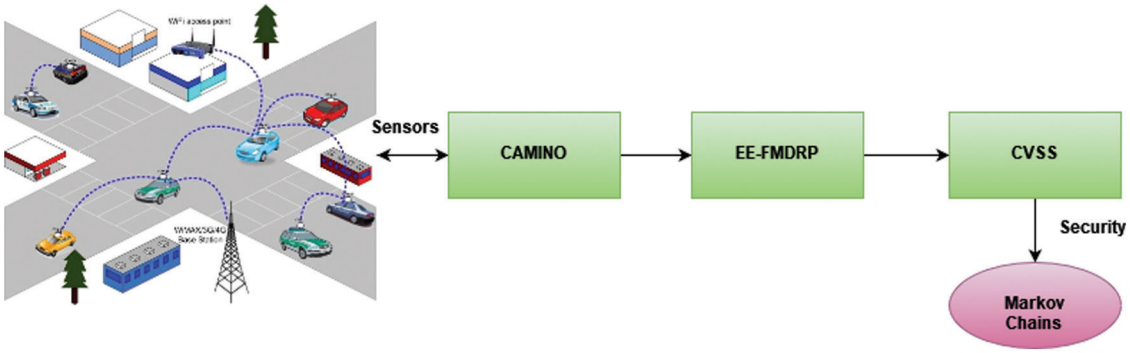

Figure 1: Overall architecture of CA-EEFP-CVSS

The message Controllers is indeed an element in the CAMINO-Core design which is in charge of overseeing the C-ITS signals which are received by the applications through the network engineering which are enabled. The standard of a reasonable will determine how communications first from applications were translated to the transmitters. The services id is sent by the message Controllers to be utilized as parts of Basic Transport Protocol (BTP) headers in the ITSG5 and C-V2X PC5 transmitter and Bluetooth components, or even in the subject again for Message Queuing Telemetry Transport (MQTT) transmitter. Its communication Processor would relay and analyze data collected by the transmitters via the data link. The Communication Manager will route the signal to the materials delivered depending on the service identity extracted first from BTP headers or MQTT subject. Fig. 2 depicts the CAMINO platform's design. CAMINO supports C-ITS operations in a dynamic, modular manner and supports hybrids connectivity by interacting with such a range of various segments.

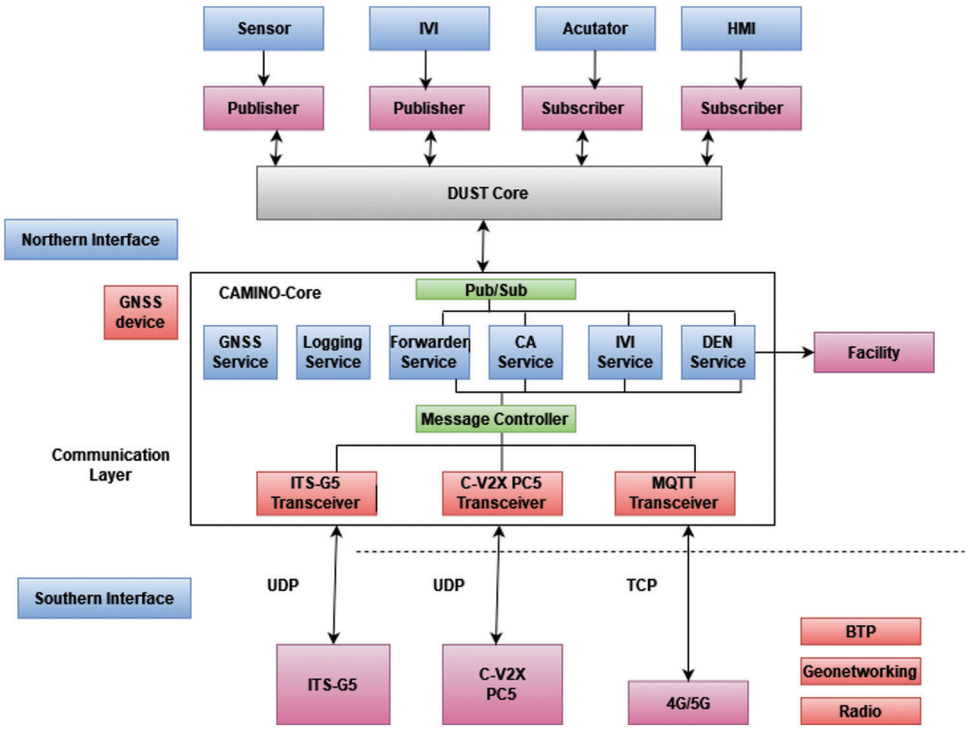

Figure 2: Structure of CAMINO architecture

Various V2X wireless communications components could be attached to the CAMINO-Core through specific connections. The interfaces of the components connected to the device which operates the CAMINO-Core may vary. The C-ITS solutions may intelligently and flexibly transfer same information across much connectivity. For instance, depending on the desired operating condition, the CAMINO-In-Vehicle Core's Sign services may transmit Interchangeable Virtual Instrument (IVI) signals through ITS-G5, C-V2X PC5, and/or 4G. Furthermore, the same produced information can be simply broadcast in parallel across several platforms. The CAMINO-Core may handle incoming messages via numerous communications channels at the receiver section. Different communications methods are supported, allowing for flexibility evaluation of C-ITS systems across different V2X wireless standards. Moreover, it could provide communications redundancies by intelligently carrying information across several platforms given current natural conditions (e.g., link quality, congestion, interference,). The connection route is presently determined based on design parameters. Including a smart optimization method may increase the communication's efficiency even more, and scientific investigations may look into it [1].

3.1.1 Communication Between Direct-Short Ranges

The European telecommunication standard institute (ETSI) ITS-5G protocol and the mobile network C-V2X PC5 technologies were already being deployed for straight quick communications inside the designated 5.9 GHz ITS radio occurrence. The CAMINO theory presupposes that what a specialized business component handles real sending and receiving for every technology. The V2X wlan components handle the bottom tier of an ETSI ITS architecture, like the Basic Transport Protocol (BTP), Geonetworking, and radio levels, whereas CAMINO-Core manages the facilities level. The business components set the wireless characteristics (e.g., channels, signal strength, broadcast variety, and so on).

3.1.2 Communication on Cellular Long-Range

CAMINO enables wireless long-range connectivity employing 4G and even 5G radios, often referred to it as C-V2X Uu, wherein Uu relates to a connection in use for connectivity between the UE and the central node, in additional too quick techniques. A routing protocol web connection is provided by the mobile connection. An Application program in CAMINO-Core allows messages to be sent to a Middleware, which can be on the edges or even in the center. The very same facilities level communications created by the CAMINO-Core functions (see Section 4) can now be shared on particular subjects through the Server component. The MQTT client supports multiple subjects and therefore can route new messages to an appropriate system. GeoCasting systems might be utilized to variety of frequencies to automobiles that used a geo-tiling technique, in which people received relevant data to their tile instantly. Moreover, CAMINO-forwarder System's capability provides again for open transfer of data sources.

3.1.3 C-ITS Modules in Camino

Many facilities activities have been specified used by ITS systems as parts of an ETSI C-ITS standards, including CA, decentralized environmental notification (DEN), IVI, Stoplight Manoeuvrability (TLM), Traffic Light Control (TLC), and much more. CAMINO-Core presently has a minimal version of CA, DEN, and IVI, which supports broadcast and receipt of CA-Message, Decentralized Environmental Notification Message (DENM), and Infrastructure to Vehicle Information Message (IVIM). The Vanetza library an accessible version of the ETSI C-ITS protocol stack, is used to build the applications.

Any one of these programs will automatically begin when the CAMINO-Core is started, based just on settings. With such, before messaging frequency, each operating application will start delivering messages. According to ETSI and International Standard Organization (ISO) standards, the Computer-Aided Manufacturing (CAM), DENM, and IVIM signals are Abstract Syntax Notation One (ASN.1) encrypted. Tab. 1 shows an overview of the available requirements. If the information is now to be conveyed using one of the short range network interfaces, a headers carrying a so-called "service identifier" is inserted

once it is forwarded to the southern interface via the Message Controller and Transceiver modules. Since such communications are obtained from of the southern interface, the resource identification is used to route them to the materials delivered. CAMINO doesn't really include additional prefixes to the message for lengthy connection, instead using various MQTT subjects to distinguish between the various applications.

Table 1: Different specifications of C-ITS [1]

C-ITS Applications	Versions
CAM	ETSI EN 302 637-2 V1.4.1 and ETSI EN 302 637-2 V1.3.2
DENM	ETSI EN 302 637-3 V1.3.1 and ETSI EN 302 637-3 V1.2.2
IVIM	ETSI TS 103 301, version 1, 2016, ISO/TS 19321:2015

3.1.4 Sensors, Actuators and Integration of External Services

CAMINO-Core is linked only with DUST platform and use a publisher/subscriber structure just at northern interface. Inside a contemporary IoT system, DUST optimizes redistribution of wealth. DUST messages allow distinct software applications to transmit information to each other employing the DUST platform's central, DUST-Core. The fundamental gateway setup has to be replaceable because the parts have to be able to travel across platforms. To incorporate the DUST structure into the CAMINO template, we created a set of publishing houses which can be used to stimulate additional services at CAMINO-Core based on information from a Can BUS or even the vehicular Unit (RSU) sensor systems, as well as a set of subscribers which brought data from the various ITS facilities inside the car. Such data could be utilized to control an actuators (e.g., for driverless cars) or visualized to use a graphical user interface (GUI).

It designed a DUST publisher again for IVS business application which enables automobiles real-time accessibility on digital road signs situated on front of gates across Belgian motorways. Towards this purpose, we created an app that regularly retrieves road signs information from of the Belgian Govt's data base, acting as an objective third network operator. The DUST publisher analyzes the data based on the necessary setup parameters and prepares a JSON statement that contains all crucial data, such as the road sign per lanes, the tower locations, the time whenever the signal was changed, and etc. The CAMINO-Core implementation operating on every RSU receives this signal and sends it out.

3.1.5 Logging Features of Camino-Care

Every communications delivered and collected through the southern Interfaces first from various modern communications components are logged by the CAMINO-Core software (ITS-G5, C-V2X PC5 and Cellular modem). All data is kept in accessing and monitoring just on machine in which the CAMINO-Core is executing. For prevent resetting any one of the local database log-files, a new log directory is created each time the CAMINO-Core program is launched, with the present timestamp as the folder title, <yyyyMMDDTHMMss>. For demonstration purposes, log-data can be pushed in real-time to a remote database, however it was not advised for assessment because log-data could be lost if the remote link fails.

CAMINO-Core could log these latest details:

- CA, IVI, DEN functions and redirected communications were sent or received through the southern interface (ITS-G5, C-V2X PC5, 4G/5G).
- Positioning-speed information recorded first from GNSS • Incoming/outgoing communications via the northern interface

The InterCor recording standard is used in all information collected by CAMINO-Core just on southern, including captured order to improve.

3.2 Framework of EE-Fmdrp

In the work, most automobiles are assumed to have been enrolled with the transportation management authorities utilizing respective Ids, who manage all automobile personal information. Responsive signal communications are sent to adjacent vehicles when the vehicles are in a particularly affected. EM ID (emergency message ID), role of origin vehicles, travel speed, orientation, and duration are all included in the urgent signal. Its orientation, location, range, and velocity of the cars are employed in this proposed scheme to detect the vehicles at the next in order to transmit the urgent messages to a specific truck. This protocol uses three kinds of communication links: vehicle-to-vehicle, vehicle-to-RSU, and RSU-to-RSU. Fig. 3 depicts the energy-efficient-quick delivery of messages flexible network structure.

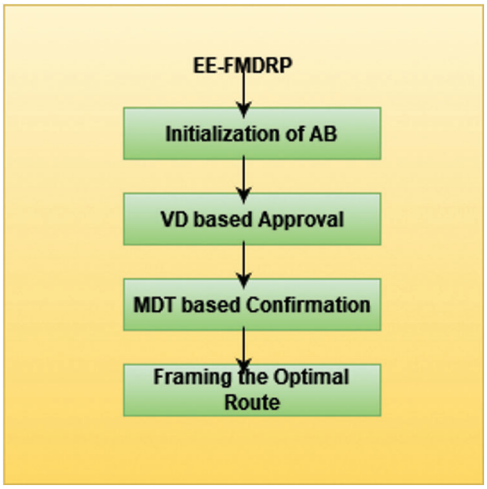

Figure 3: Framework of EE-FMDRP

3.2.1 Initialization of Adaptive Beaconing (AB)

The fundamental goal of adopting adaptive beaconing (AB) is to communicate experience and understanding information by frequently sending beacons, resulting in much less congested wireless link. It can be accomplished by estimating two aspects: the transmission format's reliability and the statement's effectiveness. It aids inside the improvement of the traffic data system's performance. The procedure of AB startup is discussed in this section.

Even during procedure, the automobile at the sender side spreads the urgent beacon message to the terminals in the communication area that surrounds the origin. Over a certain transmission area, the neighbor collection [NBs(VEx)] consists of the adjacent nodes of automobile VE. A vehicle is chosen from the neighbor set [NBs(VEx)] when the vehicle begins forwarding the beacon signal. The startup procedure begins with a communication link being sent to all of the vehicles. Endpoints in the [NBs (VEx)] satisfy the criterion that they are in the transmission range. Because the nodes are very dynamic, the invoking function called at frequent intervals to modify the current neighbours. The process for AB activation is shown in Algorithm 1.

Algorithm 1: Initialization of AB

Start

Initialize the Adaptive Beaconing AB

X is the resource vehicle

NBs (X) ε VE → Neighbor vehicle position present in the resource vehicle 'X' between the range of message area.

// NBs is the message collection between the Neighbour vehicle position

// VE→ Vehicle position {VE1, VE2, VE3,…, VEn}

For each

y ε NBs (X)

Node 'X' forwards call request to node 'y'

End For

3.2.2 Vd Based Approval

Through emphasizing on the positioning, orientation, and directional aspects of the process, it achieves fast and efficient message distribution. The movement of automobiles on the roadway. The term vector-angle is being used here. The orientated categorization model is used to determine the vehicle's position in relation to a given area. The method for detecting location vector machine svm angles is shown in Algorithm 2.

In algorithm 2, 'SV' stands again for transmitting vehicles that intends to relay the emergency alerts, 'λ' stands for such acute predefined threshold, and 'Na' and 'Nb' stand for the neighbour group co-ordinates. The location of every car in the designated VANET, as well as its neighbouring vehicular hubs, is determined using this method, allowing for effective crisis work system.

Algorithm 2: Vehicle position detection based on vector angles

Input: VE_s, [NBs(VE_s)]

while NBs (VE_s) $\neq \varnothing$ do

for a=1 to num [NBs(VE_s)], m=1 do

$NBs(VE_s) = NBs(VE_s)\text{-}\{N_a\}$→eliminate N_i from $NBs(VE_s)$

$R_M \leftarrow N_a \Rightarrow$ sort N_a into directional area R_M

for b=a to num [NBs(VE_s)] do

If (N_a SV N_b<λ) then

$R_M \leftarrow N_b \Rightarrow$ keeps the similar R_M of N_a

$NBs(VE_s) = NBs(VE_s)\text{-}\{N_b\}$

End if

b++

end for

store R_M into segment buffer

d++

end for

end while

3.2.3 Authorization Based on VD

The direction of moving vehicles can be used to determine whether or not the present automobile is travelling towards the objective. The ideal intermediaries, known as advancing neighbor, could be predicted using this information. Vehicle set VE1, VE2, VE3,…, VEn, which is permanent, symbolizes the automobile networks, so every automobile has the capability to identify whether this is moving more in the direction of the targeting pod or otherwise. According to a proximity study seen among current and the past, the answer is still no vehicles, as well as the originating cars.

The vehicles just at reception point discover the speed rates as Dist in the AB set intervals (T_{AB}). The range between the vehicle node and the source node is indicated as Dist at any particular time (T). The set of equations are used to determine the direction of a passing car.

$$VD = \begin{cases} 1, & if\ Dist(T_{AB}) > Dist\ (T) \\ 0, & Otherwise \end{cases} \tag{1}$$

Whereas if answer is 1, the criteria is true, and this is assumed that current vehicle unit is travelling inside the direction of the target. The criterion also isn't met if an outcome is 0. As a result, the automobile is moving in the opposite direction of the needed movement.

Furthermore, during the vehicle direction (VD) based permission stage; the automobile aims to decide why not to engage in communication delivery as just an ideal forwarded neighbour in order to obtain permission. Whenever the VD is 1, the node is driving towards to the destination, it gets a call request, and it replies to the source node with a message called call request approval, as shown in the above equation for finding the vehicular path. However, if it gets 0, the response from of the present vehicle to a source will be call demand refusal. A request approval list (RAL) and a demand confirmation list (RCL) are maintained by all vehicular nodes that participate in VANET communication (RCL).

3.2.4 Confirmation Based on Message Delivery Time (MDT)

The method of sending neighbour identification is simplified by the assessment of communication time delivery. The information arriving duration to the vehicle directly can be analyzed by calculating MDT. Depending on this, the vehicle node does have the ability to locate the best sending neighbors for effective and fast propagation of messages. As a result, Message Delivery Rate (MDR) is assessed using Eq. (2).

$$MDT = \frac{Dist(VE)}{Speed\ (VE)} \tag{2}$$

If you're looking for a supply car, you've come to the right place acquires at most a identify demand approval reply; it can be chosen as being one of the finest forwarding neighbors, which would be located further away first from originating automobile and competent of dispersing communications with a short message delivery time. A Lower MDT (LMDT) stands for

$$LMDT = \min(MDR_{Me}),\ \ \mathrm{M} = \ 1,\ 2,\ 3,\ \ldots,\ \mathrm{n} \tag{3}$$

Here, MDR_{Me} represents the information passing duration of vehicle node 'M'.

3.2.5 Optimal Route Framing

The call request confirmation response is transmitted by the mobile nodes, which establish the path. That really is, the path design was performed by linking the hubs that have been chosen as the best intermediary for transmitting emergency alerts quickly and efficiently. A network 'M' sends a call request confirmation message to the node 'N' at first. The path structuring is then started by the nodes 'M.' the verified cars are kept to a travel path until the target automobile is reached. As a result, in the event of an emergency,

the EE-FMDRP concept constructs an energy efficient routing by analyzing the distribution nature of the vehicularnodes.

3.3 Markov Chain Based Security Authentication and Vulnerability Scores

Here the results serve as initial contribution to our Markov Chain model's probability estimates for position change. Our empirical intrusion prevention assessment approach is described. The Markov Chain model's next key is targets of hackers, which contain assets for intrusion prevention evaluation.

3.3.1 Cvss Parameters

A designation "remotely" (Re) for the Access Vector (AV) in each and every class is enabled by the connection of the IoV architecture components. Each area except networking falls into the "high" area when it comes to Access Complexity (AC) (Hi). The reason for choosing this topic is because CAV is a security technology that necessitates the strictest access control measures at all times. Because attackers have immediate access to multiple based on service computer networks, network AC stays "low" (Lw) in the based on service situation.

In terms of authentication (Au), technology by definition provides additional accessibility and establishing a secure connection. Accessibility to the IoV server and car environments "needs" (Re) login, although public infrastructure like GPS data receipt "doesn't" (NRe) verification. Excluding the data domain, each subcategory necessitates authentication principles. Satellites are not always authenticated by standard Gps devices. A program that runs inside data receiving ports, on either hand, verifies that the data are valid.

Compromised technique has the ability to compromise the program's "full" (Con) confidentially, security, and reliability. Similarly, if information or network users are not appropriately discovered in initial checks, effective information and connection security tampering may enable them to proliferate through the network. However, there will be a negative influence on incomplete (Pa). When it comes to the Impact Bias (IB) and the local web situation, information and communication elements prioritize "integrity" (In) over the other needs, because faulty geographical information or connection objects can degrade the system.

Because there is a centralized inertial sensors software component, the IB of technology gives "available" more importance (Ab). In terms of the hardware category, abusing any of the specified security requirements results in a similar "normal" (N) impact to the business. Previous research on GPS faking provides a "proof of concept" (PoC) for manipulating position information in terms of information threats. That feature could be used to infer the presence of other "unverified" (UCB) authorities supporting the study's credibility (RC). At a certain period, "temporal fix" (TF) options exist again for prediction and mitigation of these threats just at Remediation Level (RL).

This is important to compute the total CVSS ratings Basis Factor (BS), Temporal Score (TS), and Environmental Score (ES) all with criteria mentioned (ES). The primary CVSS results are computed using formulas 4, 5, and 6 that can be seen in which the Confidential Effect Bias (CIB), Integrity Impact Bias (IIB), and Availability Impact Bias (AIB) scores are dependent on the IB settings.

$$\mathrm{BS} = 10 \cdot \mathrm{AV} \cdot \mathrm{AC} \cdot \mathrm{Au} \cdot ((\mathrm{CI} \cdot \mathrm{CIB}) + (\mathrm{II} \cdot \mathrm{IIB}) + (\mathrm{AI} \cdot \mathrm{AIB})) \tag{4}$$

$$\mathrm{TS} = \mathrm{BS} \cdot \mathrm{Er} \cdot \mathrm{RL} \cdot \mathrm{RC} \tag{5}$$

$$\mathrm{ES} = (\mathrm{TS} + (10 - \mathrm{TS}) \cdot \mathrm{CDP}) \cdot \mathrm{TD} \tag{6}$$

3.3.2 Verification Model of Quantitative Security

For illustrate the usefulness of expanded Markov Chain modeling on attacker propagating networks which match the classification patterns of the 4 + 1 perspective model analysis, a somewhat simplified version of the attacker realization meter and technique in can be used. The notion that such expanded Markov Chain provides sufficient in representing the low assault phases of our IoV use scenarios is the rationale for not relying on non-homogenous continuous-time Markov models.

A finite condition in time domain The Markov Chain is a continuous space and place random system in which prospective values at period ti + 1 are determined only by actual rates at moment ti, with no reference to prior values at moment ti1. The Markov Chain M C(I, PM, A) is a three-tuple that includes the network subspace I, the conditional probability matrices P, and a range of possible nuclear operations A. We set E = 1 because we presume no blank act impacts the realization measure E. To make things even easier, all ratios of a condition to goal likelihood can be removed. Their focus in worst attack with maximal impact is the rationale for this. As a result, phase changes which link the beginning and destination stages with diversions are maintained. As a consequence, the essential factors are taken into account: (1) condition, (2) transitioning, (3) actions, and (4) overall condition to goal possibility.

1. SI ∈ I, for which the condition SI holds a few of the viewing models viewpoints' identifiers of HW, SW, Net, or Information.
2. $\sum\infty$ j=1 pij = 1, ∀p ∈ PM.
3. The chances of assault vectors and protection events are ai, di A.
4. W n(SI=1) = $^{\Sigma}_{SI\in SUBSEQ(S1)}$ pij. $W^{n-1(SI)}$, where SUBSEQ proceeds the set of outstanding states SI.

4 Result Analysis

The NS-2.34 software is used to test the efficiency of proposed CA-EEFP-CVSS method. This model setting was created to manage message distribution in real emergencies on main roads and in a track system. Results were compared with previous methods including such emergency message dissemination for vehicles (EMDV) and traffic emergent game play routing protocol (TDBRP) and CVSS for VANET, in order to show the effectiveness of the CA-EEFP-CVSS. Tab. 2 lists the most important model parameters, along with actual results. The vehicle units are said to be moving at randomly. Its targeted automobiles are parked along the side of the highway.

Table 2: Simulation parameters

Parameters	Values
Simulator	NS-2.34
Simulation area	3000 m × 2900 m
Simulation time	250 s
No. of roads	36
No. of junctions	22
No. of vehicles	250
Vehicle speed	Random
MAC protocol	802.11 DCF
Capacity of channel	2 Mbps
Packet size	128 byte

4.1 Evaluation of Transmission Delay

It was assessed using key VANET metrics including such average packet, bandwidth, communication excess, energy usage rates, and transmission time. That long it takes for a signal to produce the desired automobile from of the sender side is commonly referred to as network latency. The model accounts again for time it takes to distribute and re-distribute alert messages. The suggested CA-EEFP-CVSS method achieved lower communication delays than some other comparable systems, as shown in the chart.

Fig. 4. shows the transmission delay of the proposed CA-EEFP-CVSS method. The proposed CA-EEFP-CVSS achieves 2.6 sec and the existing methods achieve EMDV 8.49 sec, TDBRP 3.2 sec, CVSS 5.6 sec. It outperforms better than the existing systems.

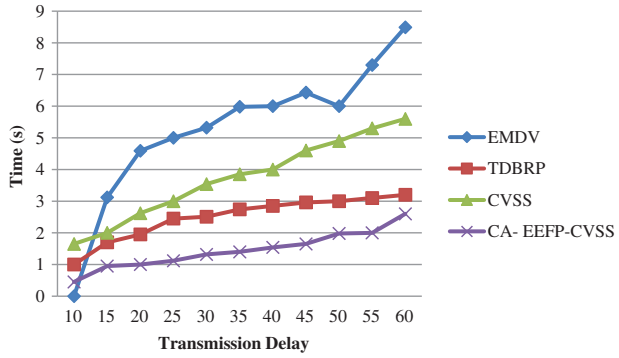

Figure 4: Evaluation of transmission delay

4.2 Evaluation of Throughput

The throughput results obtained, that are described as the information packets sent to the specific vehicle per seconds. The proposed model has a higher throughput than the others, as indicated in the image. As a result, urgent communications are delivered to their intended recipients in a timely manner. This suggested framework gets a greater throughput ratio and continues to increase with respect to time, as shown in the figure. The CA-EEFP-CVSS achieves an 8 percent increase in throughput over earlier work.

Fig. 5 shows the throughput of the proposed CA-EEFP-CVSS method. The proposed CA-EEFP-CVSS achieves 11.65% and the existing methods achieve EMDV 5.0%, TDBRP 6.5%, CVSS 8.7%. It outperforms better than the existing systems.

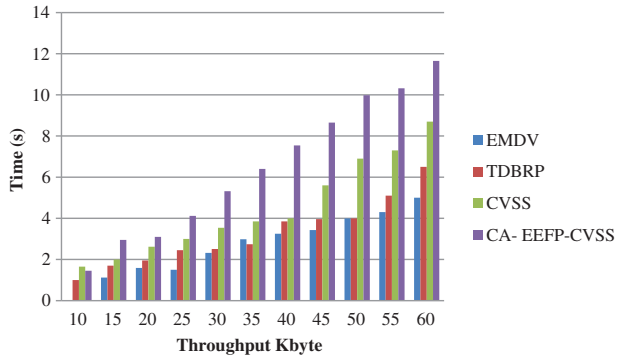

Figure 5: Throughput

4.3 Evaluation of PDR

Furthermore, the system's effectiveness has already been assessed by calculating the packet delivery ratio (PDR), which is calculated as the proportion of packets received by endpoints toward those produced by origins, and is dependent on vehicular traffic and movement speed, respectively.

Fig. 6. shows the Packet delivery ratio of the proposed CA-EEFP-CVSS method. The proposed CA-EEFP-CVSS achieves 95.78% and the existing methods achieve EMDV 82%, TDBRP 88.89%, CVSS 92%. It outperforms better than the existing systems.

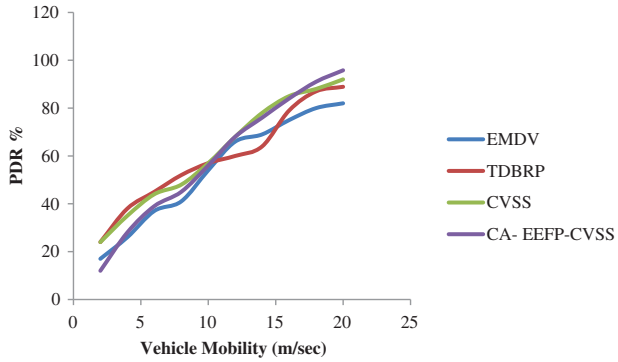

Figure 6: Packet delivery ratios

4.4 Energy Consumption

Power consumption would be another significant issue to consider when evaluating the developed system's effectiveness. Furthermore, the energy consumption rate is defined as the ratio of a vehicle node's total energy consumption to the total number of packets transmitted. The study has been done in this case based on the vehicle's ideal speed. The findings are given in a report.

Fig. 7. shows the energy consumption of the proposed CA-EEFP-CVSS method. The proposed CA-EEFP-CVSS achieves 17% and the existing methods achieve EMDV 47%, TDBRP 20%, CVSS 42%. It outperforms better than the existing systems

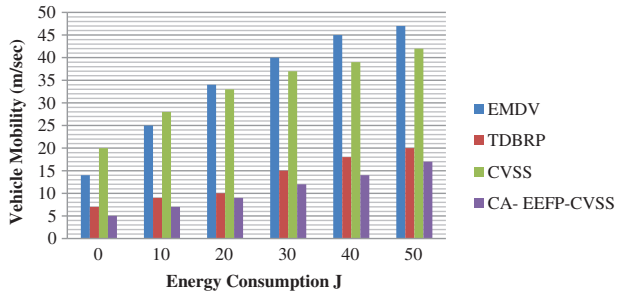

Figure 7: Energy consumption

5 Conclusion

The CA-EEFP-CVSS structure is a flexible hybrid V2X networking system for CCAM applications. This is suggested in this study to provide an intelligent vehicular infrastructure using hybrid common vulnerability scoring system and fast message routing protocol. CAMINO is intended to be a flexible method for implementing a variety of automotive communication networks and the applications that built

on windows of it. The produced information gets sent in a variety of ways using one or more V2X technology, boosting communication system and improving reliability of the network. Moreover, the CAMINO platform is ITS hardware neutral, which means it may run on any sort of stations, including OBUs, RSUs, UEs, computers, and so on. Robust monitoring features allow for the gathering of useful data that can be used to monitor the efficiency of V2X technology and the applications that operate on front of it. The proposed system uses hybrid Co-operative, Vehicular Communication Management Framework (CAMINO) and Energy Efficient fast message routing protocol with Common Vulnerability Scoring System (CVSS), methodology for improving the vehicular networks. This authorization used for information transmission period of given time and that verification is predicted. As a result, there is indeed a set of automobiles in the confirmation list that are deemed to be the best mediums. The directional and time-based prediction efficiently consumes less energy. The most power path for exchanging packets has indeed been established using the vehicular node in the verification table. The simulated results were observed using a variety of factors in order to demonstrate the EE-efficacy. The CA-EEFP-CVSS method outperforms in terms of shortest transmission latency achieves 2.6 sec, highest throughput 11.6%, and lowest energy usage 17% and PDR 95.78%. The proposed system provides security and also finds the shortest path during emergency cases.

In future advanced artificial intelligence and machine learning methods will give better performance in the wireless vehicular networks. These methods will helps to improve the security level of the system and help to detect the shortest route.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of the paper.

References

[1] D. Naudts, V. Mgloginnis, S. Hadiwardoyo, D. Den Akker, S. Vanneste *et al.,* "Vehicular communication management framework: A flexible hybrid connectivity platform for CCAM services," *Future Internet*, vol. 13, no. 81, 2021.

[2] Z. Machardy, A. Khan, K. Obana and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, pp. 1858–187, 2018.

[3] J. Lauinger, M. Aslam, M. Hamad, S. Raza and S. Steinhorst, "Quantitative system level security verification of the IoV infrastructure," *arXiv preprint arXiv, 2101.06137*, 2021.

[4] K. Satheshkumar and S. Mangai, "EE-FMDRP: Energy efficient-fast message distribution routing protocol for vehicular ad-hoc networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3877–3888, 2021.

[5] A. Costandoiu and M. Lebatelligent, "Transport systems (ITS), radio communications equipment operating in the 5855 MHz to 5925 MHz frequency band; harmonised standard covering the essential requirements of article," *IEEE Access*, vol. 2, no. 3, 2019.

[6] R. Jacob, N. Franchi and G. Fettweis, "Hybrid V2X communications: Multi-RAT as enabler for connected autonomous driving," in *Proc. 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications(PIMRC)*, Bologna, Italy, pp. 1370–1376, 2018.

[7] X. Xu, Z. Zeng, Y. Wang and J. Ash, "A framework of a V2X communication system for enhancing vehicle and pedestrian safety at un-signalized intersections," in *Proc. International Conference on Management Science and Engineering Management*, Melbourne, Australia, pp. 51–63, 2018.

[8] T. K. Lee, T. W. Wang, W. X. Wu, Y. C. Kuo, S. H. Huang *et al.,* "Building a V2X simulation framework for future autonomous driving," in *Proc. Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Matsue, Japan, pp. 1–6, 2019.

[9] F. A. Schiegg, J. Krost, S. Jesenski and J. Frye, "A novel simulation framework for the design and testing of advanced driver assistance systems," in *Proc. IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, Honolulu, HI, USA, pp. 1–6, 2019.

[10] S. Jeong, Y. Baek and S. H. Son, "A hybrid V2X system for safety-critical applications in VANET," in *Proc. IEEE 4th International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA)*, Nagoya, Japan, pp. 13–18, 2016.

[11] R. J. Makwana, "An algorithm EMD for emergency in VANET," *International Journal of Computer Science Engineering and Technology*, vol. 6, no. 06, 2011.

[12] M. Torrent Moreno, J. Mittag, P. Santi and H. Hartenstein, "Vehicle-to-vehicle communication: Fair transmit power control for safety-critical information," *IEEE Transactions on Vehicular Technology*, vol. 58, pp. 3684–3703, 2009.

[13] G. Korkmaz, E. Ekici, F. Özgüner and U. Özgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in *Proc.1st ACM International Workshop on Vehicular Ad hoc Networks*, Philadelphia, US, pp. 76–85, 2004.

[14] M. Mangai and S. Tamilarasi, "A vehicle monitoring and traffic collision avoidance system using ILCRP-IDS in VANETS," in *Proc. National Conference on Telecommunication in Health Care Engineering*, Erode, India, 2011.

[15] S. Rizvi, J. Willet, D. Perino, S. Marasco and C. Condo, "A threatto vehicular cyber security and the urgency for correction," *Procedia Computer Science*, vol. 114, pp. 100–105, 2017.

[16] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, 2017.

[17] P. Karkhanis, M. G. Van Den Brand and S. Rajkarnikar, "Defining the C-its reference architecture," in *Proc. International Conference on Software Architecture Companion (ICSA-C)*, Stuttgart, Germany, pp. 148–151, 2018.

[18] M. Lu, R. Blokpoel, M. Fünfrocken and J. Castells, "Open architecture for internet-based C-ITS services," in *Proc. 21st International Conference on Intelligent Transportation Systems (ITSC)*, Maui, HI, USA, pp. 4–7, 2018.

[19] R. Riebl, C. Obermaier, S. Neumeier and C. Facchi, "Boosting research on inter-vehicle communication," in *Proc. 5th GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2017)*, Nürnberg, Germany, pp. 37–40, 2017.

[20] S. Vanneste, J. Hoog, T. Huybrechts, S. Bosmans, R. Eyckerman *et al.,* "Distributed uniform streaming framework: An elastic fog computing platform for event stream processing and platform transparency," *Future Internet*, vol. 11, no. 158, 2019.

[21] J. A. Larcom and H. Liu, "Modeling and characterization of GPS spoofing," in *Proc. IEEE International Conference on Technologies for Homeland Security (HST)*, Boston, USA, pp. 729–734, 2013.

[22] S. M. Abraham, "Estimating mean time to compromise using non-homogenous continuous-time markov models," in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, USA, vol. 2, pp. 467–472, 2016.