International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/02 Volume 12, Issue 1, January – February (2025)

RESEARCH ARTICLE

Enhancing 5G-VANET Environments with SDN-Based Package Filtering for Improved Networking

P. Dharanyadevi
Department of Computer Science Engineering, Puducherry Technological University, Puducherry, India.
✉ dharanyadevi@gmail.com

Amirthasaravanan Arivunambi
Department of Computer Science, Pondicherry University, Puducherry, India.
aasaravanan777@gmail.com

B. Senthilnayaki
Department of Information Technology, St. Joseph's Institute of Technology, OMR, Chennai, India.
nayakiphd@gmail.com

Pethuru Raj
Edge AI Division, Reliance Jio Platforms Ltd, Bangalore, India.
peterindia@gmail.com

Received: 19 October 2024 / Revised: 11 January 2025 / Accepted: 24 January 2025 / Published: 28 February 2025

Abstract – This research explores the integration of Software-Defined Networking into 5G-enabled Vehicular Ad Hoc Networks (5G-VANETs) with a focus on the implementation of a package filtering model. The goal is to enhance networking within these dynamic environments. By leveraging SDN's centralized control capabilities, this study aims to optimize network performance, enhance security, and improve the quality of service in 5G-VANETs. The outcomes of this research have the potential to contribute significantly to the advancement of intelligent transportation systems and vehicular communication networks. As the VANET milieu operates dynamically, the major issues are to afford high reliability, low latency, and high bandwidth. 5G significantly provides seamless connectivity and ultrafast speed for vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications. Advancements in internet of vehicle brought few security issues such as illegal device access, data injection, and man-in-the-middle attacks. To avoid these issues, this work implements the Package Filtering Model (PFM) that is trained using machine learning and ready to use for real-time detection. It filters out the fraudulent transaction based on the frequency and behavioural characteristics of the communication. The simulation results ensure that the proposed mechanism affords enhanced packet delivery, lower transmission delay, minimum fraud package, and bare minimum block processing time compared to the existing state-of-the-art mechanisms.

Index Terms – VANET, 5G, Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), SDN, Package Filtering Model, Machine Learning, Performance.

1. INTRODUCTION

5G is a global wireless network standard after 4G that affords massive network capacity, consistent user experience, ultra-low latency, promising speed, and increased availability. 5G can potentially change industries with its high speed and reliability [1]. This transformation can be seen in terms of IoT, where large numbers of embedded systems can interconnect with any electronic device, and this will promise a scaled-down data rate, cost per bit, and latency.5G technologies provides the necessary infrastructure to support the diverse and demanding communication requirements of Vehicular Ad-Hoc Network (VANET), making it a promising choice for improving road safety, traffic efficiency, and transportation services in the future [2].

Internet of Vehicles (IoV) aims to facilitate vehicles to communicate with their human drivers, roadside infrastructures, pedestrians, and other vehicles [3]. The data communication in the Software Defined Network (SDN) based 5G-VANET (S5V) milieu is handled by IoV, a distributed system [4]. The vital deployment of IoT and smart city uses a VANET, which is a technology that can communicate with V2I (Vehicle to Infrastructure), V2V (Vehicle to Vehicle), and V2X (Vehicle to Everything) [5]-[7]. In VANET communication, the peer improves the safety of passengers and provides information to the driver about the road infrastructure. The vehicle communicates with other vehicles which are in the range and share the road-related

RESEARCH ARTICLE

conditions and information regularly at given time intervals [8]. With the persistent development of wireless communication technologies, there is an abundant augment in vehicular applications such as financial and non-financial applications. This work focuses on the non-financial applications. The non-financial applications include traffic reporting, message sharing, sharing of the legal documents, health records, E-notary, private documents, marriage licenses, collecting taxes, and accident reports. Financial and non-financial applications' major issues are providing security among connected peers and securing sensitive data. Since VANET deals with sensitive data transmission in a network where the message passing happens with any peer, there is little way to detect that the information passed is reliable and authentic enough. The top priority should be the message's authenticity and verifying that its sender is a legitimate peer.

SDN has emerged as a promising paradigm to address the complex networking requirements of 5G-VANET environments. SDN's ability to centralize network control and dynamically adapt to changing conditions aligns with the dynamic nature of VANETs [8][9]. By integrating SDN-based package filtering, we aim to capitalize on the flexibility and adaptability of SDN to significantly improve the networking experience within 5G-VANETs. SDN eliminates the vertical integration in which the data and control plane are bundled together. SDN relies on horizontal integration, a way the two planes are separated. The control plane runs a network application above the Network Operating System (NOS) and data plane, which forwards the traffic based on how it is programmed in the control plane.

The VANET milieu should integrate with the features such that the network should support the implementation and not be heavy to slow down the transmission. There should also be a mechanism to manage, control, and operate the VANET milieu and to address the above issues; this work integrates the SDN with VANET. SDN also reduces the operational cost of the VANET by utilizing the simplified hardware, software, and management [10][11]. This work also introduces the Package Filtering Model (PFM) to filter out the suspected fraudulent transaction. PFM is a machine learning approach that can learn from its past transactions as to what a fraudulent transaction behaves like [12].

The main agenda of PFM is to detect the fraudulent network transaction happening in the network. This model is trained so that any abnormal or rapid change in information passing from one node in a minimal time could be used as a trigger fora fraudulent transaction, and many more such triggers are used to classify it as a fraudulent transaction. The world is rapidly adopting 5G technology, which is enhancing the scope of vehicle ad hoc networks in modern transport systems and is boosting the need for dependable and efficient communications within the network [13][14].

The motivation and contribution of this paper are as follows: This paper discusses modern services and applications and aims to answer world's rapidly changing digital landscape by integrating vehicular networks with the 5G technology. This paper attempts to enable seamless connectivity of the Software-Defined Networking (SDN) integrated 5G-VANET environment to the Internet, as well as improve network management and performance within mobile networks. Also, this paper proposes a Package Filtering Model (PFM) that operates in an SDN environment to prevent network attacks and thus enhances security as well as network performance. The main task is to adapt and mitigate IoT and smart transportation systems and 5G communications technologies in a way that enables high quality service and efficient security in a changing environment. As machine learning and SDN integration becomes more important for 5G-VANETs aimed at smart transportation, this work addresses potential issues of increasing the functionality and reliability of vehicular communication systems. From the simulation results, it can be seen that integrating fostered trust and security capabilities within the 5G-VANET environment greatly increases overall network performance.

The structure of the research paper is organized as follows: In Section 2, a detailed survey of relevant literature is provided, Section 3 describes the proposed 5G-VANET architecture and algorithm within the SDN-based framework, Section 4 contains the results of the experiments, and lastly, Section 5 contains the conclusions drawn from the study.

2. LITERATURE SURVEY

The integration of Software-Defined Networking (SDN) into 5G-enabled Vehicular Ad-Hoc Networks (5G VANETs) is an emerging research area focused on improving communication infrastructure in vehicular settings. Although this field is still developing, some researchers and studies have begun to investigate the use of SDN in 5G VANETs.

Indriyantol et al. [15] introduced the SDN-based VANET architecture for the heterogeneous milieu. The author validates the effectiveness of the proposed mechanism by the simulator (traffic-trace-based). Salahuddin et al. introduced an SDN-based roadside unit that migrates, mitigates, and affords cloud services. As explained by the author, the practical implementations of SDN in the context of VANET are still in its infancy [16]. Oliveira et al. implemented the SDN-based VANET by emulating the topology within Mininet-WiFi. This setup supports extended OpenFlow wireless devices with interface boards [17]. X. Ge Tao et al. introduced a solution to 5G wireless backhaul traffic by analysing traffic using small-cell and millimeter-wave communication technology [18]. Manirajet al. introduced a Machine Learning model in banking technology that is used to differentiate a fraudulent transaction based on the transaction behaviour and history of the transaction [19]. A similar concept is used in this paper to

RESEARCH ARTICLE

track down the fraudulent transactions happening in the VANET. Recent research mainly focused on the faster transmission of messages in the network, and only a few researches have been focused on security and reliability [20][21]. Hai et.al discusses how an SDN-assisted technique in heterogeneous vehicular networks can optimize route determination and guidance for information traffic, especially in scenarios involving blockages in VANETs. This approach improves traffic efficiency and reliability in complex vehicular settings [22]. Murtadha et al. identifies challenges of poor connectivity and inflexibility at high vehicle speeds and data rates. To address these, the paper proposes a flexible handover solution for VANET networks by integrating SDN and fog computing technologies. Ku et. al presented an SDN-VANET architecture that is flexible and scalable in a range of operating modes. The architecture includes local SDN agents in every vehicle to tackle possible connectivity issues with the SDN controller or Base Station (BS), improving network performance. The outcomes showed that the standard distributed architectures are not as effective as the centralized SD-VANET architecture. Nevertheless, feasible routing paths and traffic congestion management were not covered in the study [23]. Due to high vehicle mobility and the dynamic character of VANETs, link stability is essential for increasing packet delivery ratios across wireless networks, which are vulnerable to packet loss.

A unique routing strategy for Software-Defined Vehicular Networks (SDVNs) was introduced in [24] with the aim of improving link stability and performance by forwarding packets via numerous shortest pathways. Huang et al. used an SDN controller to collect detailed data on the cars in the network, including their position geographically, speed, direction, and IDs of nearby RSUs via 802.11p. OHD-SDN (Offloading with Handover Decision based on SDN) is a technique where decisions about offloading and handover are made using this information [25]. An on-demand routing strategy for SD-VANET called SDAO was presented by B. Dong et al. in a different paper [26]. It has two-level architecture: a distributed global level that lowers route computation cost, and a centralized local level that computes routes for individual cars. Furthermore, the authors of [27] put forth an SD-VANET architecture that offers flexible control, effective resource utilization, and network administration in order to facilitate next-generation (5G) communication.

This paper mainly focuses on ensuring security for non-financial applications. However, the existing approaches mainly focus on single-point failure and denial of service attacks in centralized SDNs. Furthermore, the existing approaches mainly rely on SDN for filtering packages, and if a new type of package is encountered, the rules are written in SDN. The proposed mechanism resolves the issue by using the PFM.

The motivation behind this research is to pave the way for more efficient traffic management, enhanced security, and better quality of service within VANETs, thus contributing to safer and more intelligent transportation systems. This study seeks to address the growing need for advanced networking solutions in the context of 5G-VANETs by combining the power of SDN and package filtering, with the ultimate goal of achieving improved network performance and functionality. While specific research on the integration of packet filtering within SDN for 5G VANETs is limited, the aforementioned hypothetical research topics highlight the importance of this concept in enhancing security and network management within the 5G VANET milieu. Researchers and practitioners are encouraged to explore this area further to address the unique security challenges presented by vehicular networks.

3. SDN-BASED 5G-VANET MILIEU USING PACKAGE FILTERING MODEL

The proposed mechanism is the amalgamation of critical technologies such as VANET, 5G, SDN, and machine learning. SDN makes the 5G-VANET milieu much more programmable, which controls and commands the entire milieu. SDN manages the packet routing, minimizing packet failure. Network reach ability is a critical issue in SDN, and it is resolved by the IP allocation, routing changes, policy opening, bandwidth allocation, end-to-end reachability, and service testing. Machine learning is always a step ahead of the traditional programmed system when detecting a pattern in data. It can be divided into two aspects, supervised and unsupervised, based on whether the labels are given or not. This work uses the supervised machine learning approach in developing the Package Filtering Model (PFM). Figure 1 illustrates the proposed architecture.

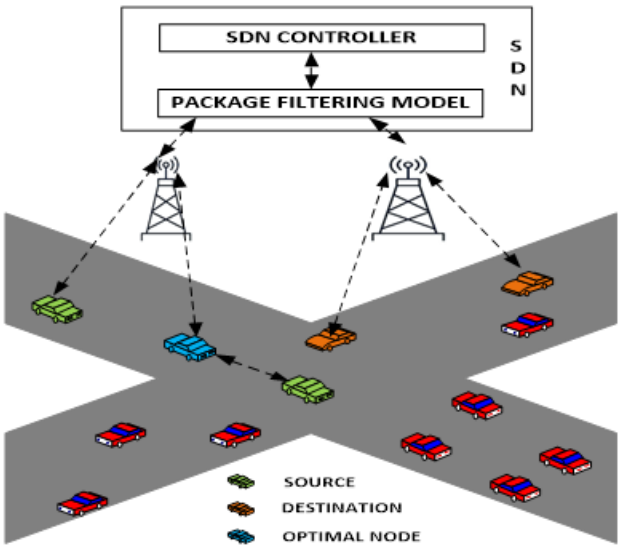

Figure 1 Proposed Architecture

RESEARCH ARTICLE

The proposed mechanism is categorized into three levels:

1. Ground Level (GL): The GL determines the initial path for package transfer.

2. Middle Level (ML): The ML filters the package using PFM in SDN and

3. Top Level (TL): In TL, the SDN controller determines the path of destination.

3.1. Initial Path Finding for Package Transfer

The sender's vehicle in the network finds a suitable path to initialize the process. Consider there are $v_1,v_2,v_3,\ldots,v_n$ number of vehicles in the milieu with On-Board Units (OBU) with the capability to act as a router. The sender vehicle transfers the package to the BS or optimal node based on the availability.

Case 1: Sender vehicle (X) and BS(Y) are withinthe same coverage area. X→Y, the X transmits the package to the Y.

Case 2: X scans for Y if there is no Y within the coverage area of X. X→A_i→Y, where A_i is the maximum number of the optimal node.

The optimal node checks for the BS within its coverage area and, if found, transmits the package to BS; otherwise, optimal node selection continues. The optimal node is selected and transmission time is calculated using Eq. (1).

$$TT_i \equiv \sum_{i}^{n} \frac{PS_i}{BR_i} \qquad (1)$$

Where, TT_i is the Transmission Time of the $'i^{th}'$ vehicle, PS_i is the Package Size of the $'i^{th}'$ vehicle in bits, BR_i is the Bit Rate of the $'i^{th}'$ vehicle in bits/second, and $n$is the maximum number of nodes in the source vehicle transmission range. As shown in Figure 2, the data is safer when the transmission time of data is lower. In this paper, the optimal node is selected based on the minimum transmission time.

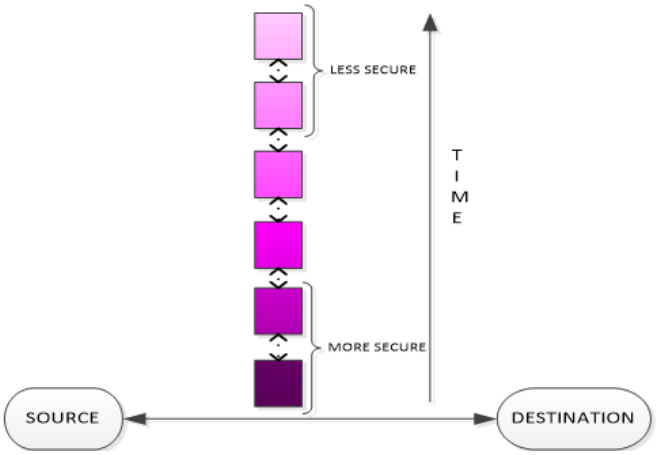

Figure 2 Packet Transfer

The packages reach the Base Station (BS), and from the BS, the package is transferred to the SDN. In SDN, the PFM filters out the packages based on how the model is trained. If the package is labeled as fraud by PFM, it is rejected.

3.2. Package Filtering Model

As per the study, the attacks in the VANET milieu are based on traffic characteristics and anomalies. This paper resolves these issues by collecting information about past transactions and establishing a database. The database includes not only the non-fraudulent transaction data but also fraudulent transaction data. This paper uses the Logistic Regression Algorithm (LRA) classification algorithm and is classified based on characteristics matching, model reasoning, and expert system. LRA maps the low dimension of non-linear separable data and projects it into high dimensional and makes it linearly distinguishable [28].

The primary task of the LRA is classifying the fraud and non-fraud package. The fraud package is denoted by 1, and the non-fraud package is denoted by 0. This paper classifies the fraud package based on these eight parameters, which are as follows:

1. Package Size (PS)

2. Sent Package Rates (SPR)

3. Speed of source IP (SIP)

4. Deviation from the mode of incoming flow packets (DFP)

5. Deviation from the mode of incoming flow bytes (DFB)

6. Package delivery time (PDT)

7. Flow Entry (FE)

8. Speed of Source Port (SSP)

PS: The package size is taken in bits, and in case of attacks, the size of packages sent is relatively smaller in size, around 200-300 bits.

SPR*:* SPR is the rate at which the packages are sent. The SPR is calculated using Eq. (2) as follows:

$$SPR = \frac{NoP}{t} \qquad (2)$$

Where *NoP* is the number of packages and *t* is the sample unit time interval.

In the occurrence of an attack, a massive number of small-sized packages is flooded into the network. If NoP increases rapidly in a given sample time interval *t*, this could be an indication of attack, and that will trigger SPR.

SIP: SIP is the total number of source internet protocol addresses sent simultaneously. The SIP is calculated using Eq.

RESEARCH ARTICLE

(3) as follows:

$$SIP = \frac{NoIP_{src}}{T} \quad (3)$$

Where, *NoIPsrc* is the source IP number, and that is transferred over the sampling time interval *T*.

In case of fraudulent transaction or attacks, a large number of forged IP addresses are generated to flood the network with data packages. Hence, the source IP number will increase drastically.

DFP: DFP is the standard deviation from the mode of incoming flow packets. The DFP is calculated using Eq. (4) as follows:

$$DFP = \sqrt{\sum_{j=1}^{N} (P_j - Mo\_P)^2} \quad (4)$$

Where *Pj* is the size of the package, and *Mo_P* is the mode of *N* packages transferred.

The *Mo_P*is determined using Eq. (4a) by:

$$Mo\_P = L + \left[\frac{f_1 - f_0}{2f_1 - f_0 - f_2}\right] \times S \quad (4a)$$

Where, *L* is the lower limit of the model class, f*1*is the frequency of the model class, *f0* is the frequency of the class preceding the model class, f2 is the frequency of the class succeeding the model class, and S is the size of the model class.

In general, the data package for fraudulent transactions is smaller compared to the normal package, and the standard deviation from mode will be smaller than normal packages, which indicates the package is malicious.

DFB: DFB is the standard deviation from the mode of incoming flow bytes. The DFB is calculated using Eq. (5) as follows:

$$DFB = \sqrt{\frac{1}{N}\sum_{k=1}^{N} (byte_k - MoB)^2} \quad (5)$$

Where $byte_k$ is the package byte, and *Mode_byte* is the mode of N bytes transferred.

The *Mo_B* is the most frequently occurring package byte, calculated using 4(a) in T period time. In an attack or fraud transaction, the DFB will be smaller than the normal transaction.

PDT: PDT is the Package Delivery Time. The PDT is calculated using Eq. (6) as follows:

$$PDT = \frac{PTH_{dist}}{P_{speed}} \quad (6)$$

Where, *PTHdist* is the distance the package has to travel and *Pspeed* is the speed at which it is traveling.

Here, PDT is the ratio of path distance to path speed, and in case of a fraudulent transaction, its value will follow a different distribution compared to PDT with normal packages.

FE: Any point in the path is considered, and the number of packages that pass through that point at some given time interval gives the flow entry. The FE is calculated using Eq. (7) as follows:

$$FE = \frac{NoP}{T} \quad (7)$$

Where, *N* is the number of packages crossing a particular point in a given time interval *T*. In a fraudulent transaction, package flow entries increase dramatically above the normal value.

SSP: Number of source ports per unit time. The SSP is calculated using Eq. (8) as follows:

$$SpSP = \frac{\sum Psrc}{T} \quad (8)$$

Where, $\sum Psrc$ is the attack source port, and *T* is the sample time interval. In case of attack, a large number of port numbers are generated.

A Python pandas data frame is created with all the above parameters as columns along with an additional column, 'TYPE', which will contain 0 or 1 to signify if the row with the associated value is fraud or not.

The system model is trained based on the past transaction, and the decision-maker model acquires the new value of the parameters such as SPF, SIP, DFP, DFB, PDT, and FE and predicts the 'TYPE'.

Let us consider $x_1, x_2, \ldots x_n$ as set of training data where each of $x_1, x_2, \ldots x_n$ is composed of above parameters with respect to a package as shown in Eq. (9). And the training data will consist of label y as well, i.e., 'TYPE' (1/0).

$$a = w_0 + w_1 x_1 + w_2 x_2 + \ldots + w_n x_n \quad (9)$$

Where, $x_1, x_2, \ldots x_n$ are the labeled training data points, and $w_1, w_2, \ldots, w_n$ are weights associated with the training data

RESEARCH ARTICLE

points. Weights $w_1, w_2 \ldots w_n$ are initialized to zero at the beginning because the cost function of logistic regression is a convex cost function that has a single optimal point, and given any starting weight it will converge to the optimal point in most of the cases.

The above value of *a* is passed to the Eq. (10),

$$y_i = \frac{1}{(1+e^{-a})} \quad (10)$$

Where, y_i represents the prediction, followed by the calculation of cost, which represents the collective loss when the algorithm makes the prediction wrongly. The goal here is to update weights $W_1, W_2, \ldots W_n$ so that in the next iteration, it does the prediction right or improves in the earlier prediction and is shown in Eq. (11).

$$cost(w) = \left(\frac{-1}{m}\right)\sum_{i=1}^{m} y_i \log(\hat{y}_i) + (1-y_i)\log(1-\hat{y}_i)) \quad (11)$$

Where y_i is the actual label and $\hat{y}_i$ is the label predicted by the algorithm and *m* represents the number of training examples.

The purpose of Logistic regression is to define a boundary or a threshold value such that the decisions are made and classes are separated based on the linear decisions. Basically, the logistic regression can be viewed as conditional probability where the previous probability of past events has an impact on the decision made in the future events [29]-[31].

3.3. Path determination by SDN

Once the package is passed through PFM, it is ready for routing, and the routing mechanism is done by the SDN controller. The SDN controller is the centralized brain control in the 5G-VANET milieu. It decides the traffic routing to destination, and the data or forwarding plane forwards the path. If congestion or data traffic occurs in a particular node, the SDN controller will immediately change the path.

In the case of VANET, nodes are mobile; package delivery is delayed with low processing and memory overhead. The classical vector routing protocols cannot be used here because of the "counting to infinity problem". The transfer is carried out with the help of an active route, forwarding node, forward route, source, and destination. An active route is a route that can be used to transfer data to the destination; only valid routes are part of an active route. The forwarding node is the node that itself is not the destination node, but the destination route goes via it, and it agrees to forward the data to the next forwarding node or destination node. Forward route is the route that will forward the data towards its destination. The source is from where the data routing is started, and the destination is the IP address to which the data is being transmitted. Algorithm 1 outlines the ground level process. Algorithm 2 details the optimal node selection procedure, while Algorithm 3 demonstrates the data filtering mechanism using PFM.

Given: n vehicles and among them k vehicles with OBU where k<=n

Step 1: Start

Step 2: Vi (vehicles) scans for the BS(BS)

If BS found

Transmit the package

Algorithm 3

Else

Step 3: Vi transmit package to nearest Vj (Algorithm 2)

End If

Step 4: Handoff begins

If

Vi leaves a network; Vi joins a nearby network and goes to Step 2.

Step 5: Stop

Algorithm 1 Ground Level

Given: 'PS' is package size in bit, 'BR' is the bit rate in bit/second, 'Di' is an array of distances from Vi.

Step 1: For each n // n is the neighbor vehicle

Calculate Transmission Time (TT): $TT \equiv \sum_{i}^{n} \frac{PS_i}{BR_i}$

End For

Step 2: Sort TT_i in ascending order

Step 3: Minimum TT = Vj

Vj=Vi

Goto Algorithm 1

End For

Step 4: Stop.

Algorithm 2 Vj Selection

Given: Package Sent Frequency (PSF), Speed of source IP (SIP), Deviation from mode of incoming flow packets (DFP),

RESEARCH ARTICLE

Deviation from mode of incoming flow bytes (DFB) and Package delivery time (PDT)

Step 1: Start

Step 2: Pass the given data in data frame format as input to the model

PFModel(input=dataframe(PSF,SIP,DFP,DFB,PDT))

Step 3: If output(PFModel)==0

Ignore the package and inform the source vehicle to resend the package

Else

Pass data to the SDN controller

End If

Step 4: Stop.

Algorithm 3 Data Filtering Using PFM

4. EXPERIMENTATION AND RESULTS

The simulation using the Network Simulator 3 (NS3) for enhancing 5G-Vehicular Ad-Hoc Networks (VANETs) with SDN-based packet filtering, follow these steps in detail: Create a VANET scenario by defining the road layout, vehicle mobility patterns, and communication ranges. In simulation the mobility generators like SUMO is used and import the generated mobility traces into NS3.NS3 doesn't inherently support SDN. To simulate SDN functionality, create custom modules to emulate the SDN controller. Create custom SDN switch modules. Define packet filtering rules within your custom SDN controller module.

These rules will determine how packets are filtered and forwarded within the SDN network. Simulate packet generation from vehicles (OBUs) in the VANET. create custom traffic generators within NS3 to model different types of applications and packet generation patterns. Implement real-time packet inspection mechanisms within custom SDN controller or SDN switch modules. This involves analyzing packet content, classifying packets, and applying packet filtering rules. Develop a mechanism for dynamically updating packet filtering rules within custom SDN controller module during the simulation.

This should reflect the dynamic nature of vehicular networks. Set up communication channels between the SDN controller, switches, and the vehicles (OBUs) within the NS3 simulation. Then need to extend existing communication models to simulate cellular or dedicated VANET communication channels. Define QoS parameters and metrics for evaluating the performance of the packet filtering system, such as latency, throughput, and packet loss, within the NS3 simulation. Generate vehicular traffic within the VANET scenario using custom traffic generators or importing mobility traces. This helps simulate various traffic patterns and congestion scenarios. Introduce security scenarios to test the effectiveness of the packet filtering rules in mitigating potential threats. This involves injecting malicious packets to assess the security measures. Implement monitoring and logging mechanisms within custom SDN controller or SDN switch modules to record and analyze network performance, security events, and rule enforcement. Run the NS2 simulation with the defined VANET scenario, SDN controller, and packet filtering rules. Collect data on network behavior, performance, and security. Table 1 illustrates the simulation parameters.

Table 1 Simulation Parameters

Simulator	NS-3.35
Simulation Area	2000m × 2000m
Mobility Traces	SUMO
Number of Vehicles	80
Vehicle Speeds	20 m/s
V2V	IEEE 802.11p
Propagation Model	Nakagami
Validation Mechanism	SDN+PFM
Control Channel Latency (typical for SDN)	5–10 ms
PFM - Rule update frequency	Every 5–10 seconds
Security Scenario	50% Fraudulent Packets

4.1. Evaluation of the Performance

The performance of the system is measured based on performance metrics such as packet delivery ratio, transmission delay, package fraud ratio, and block processing time concerning vehicle density and packet generation speed. The packet delivery ratio is calculated by the number of successful responses to the number of requests transmitted [9].

Transmission delay is calculated by the time at which requests are sent and the time at which a reply is received. The fraud packages ratio is calculated by the number of fraud packages identified to the total number of packages. Block processing time is the time taken by SDN and PFM to validate one block before transferring.

RESEARCH ARTICLE

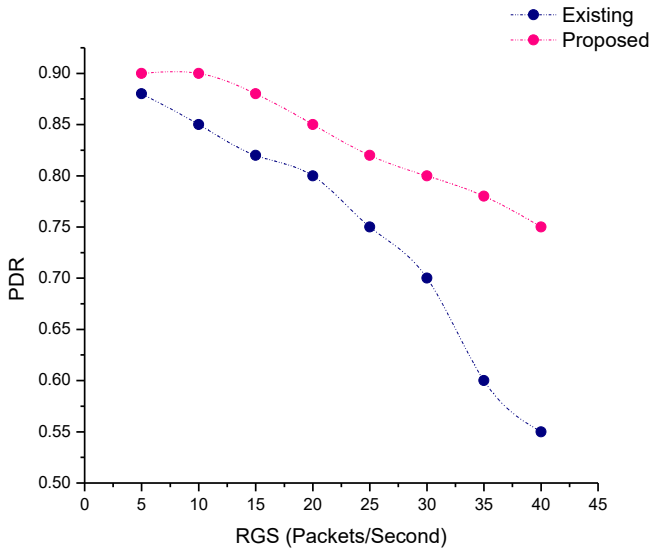

Figure 3 PDR – RGS

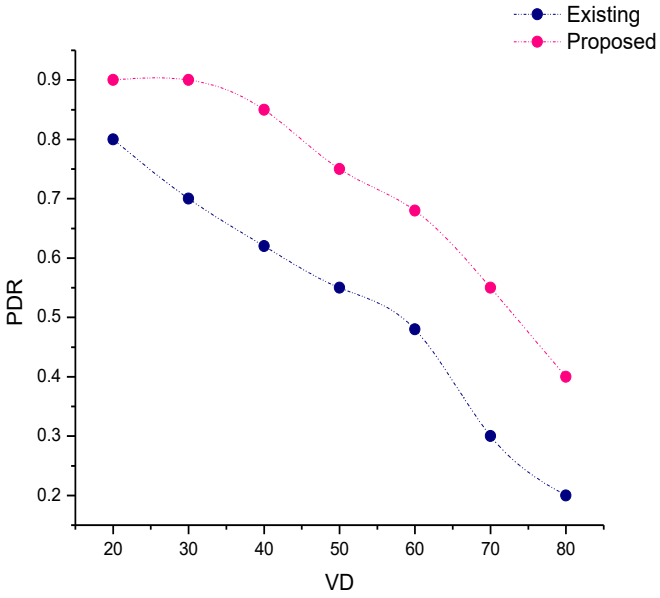

Figure 4 PDR – VD

Figures 3 and 4 demonstrate the outcomes concerning Packet Delivery Ratio (PDR) on Request Generation Speed (RGS) and Vehicle Density (VD). If less number of packages is generated, then the delivery ratio approaches 1; this could be because the levy on the networking is less. The ratio of the package received to the package sent is better when it approaches 1, and in our case, PDR is 0.75 with respect to the existing system, which has PDR=0.55. This improvement could be because of the improvement in system architecture, and the RGS is monitored. Also, in the case of Fig. 3 and Fig. 4 of RGS and VD, with the rise in the vehicles' density, the PDR is also decreased, possibly because of high network traffic. It is not the best result, but better than the existing system.

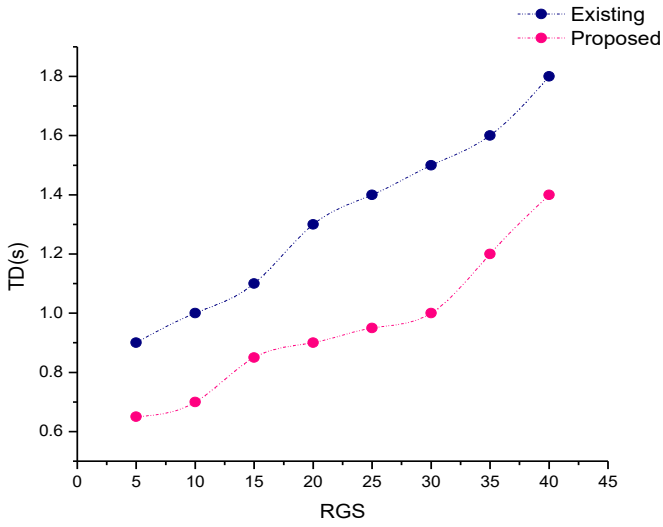

Figure 5 TD – RGS

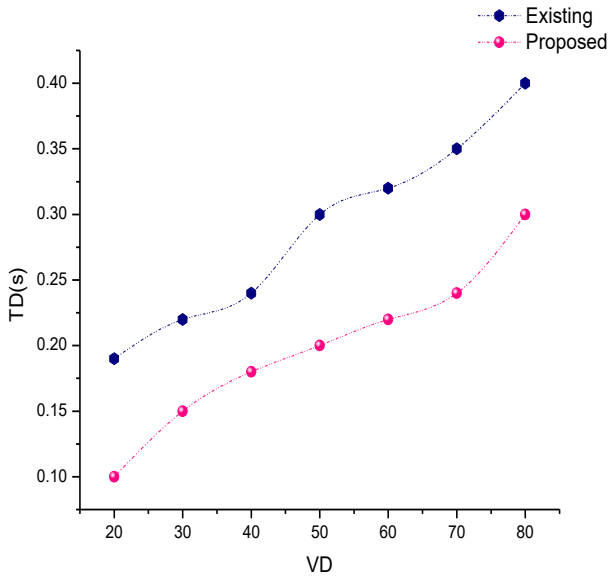

Figure 6 TD – VD

Figure 5 demonstrates the outcomes with respect to Request Generation Speed on Transmission Delay. It is natural for the graph to increase in parallel for RGS and TD because if the number of requests generated is increased, it will increase the traffic. Eventually, it will increase transmission delay.

Figure 6 demonstrates the outcomes with respect to vehicle density on transmission delay. If the number of vehicles is increased, it will increase the network traffic and RDS and TD, which maintains the proportionality in the graph. The transmission delay in both cases is less and better than the

RESEARCH ARTICLE

existing system, i.e., for VD 80, the transmission delay is 0.30 in our case, whereas 0.38 for the existing implementation.

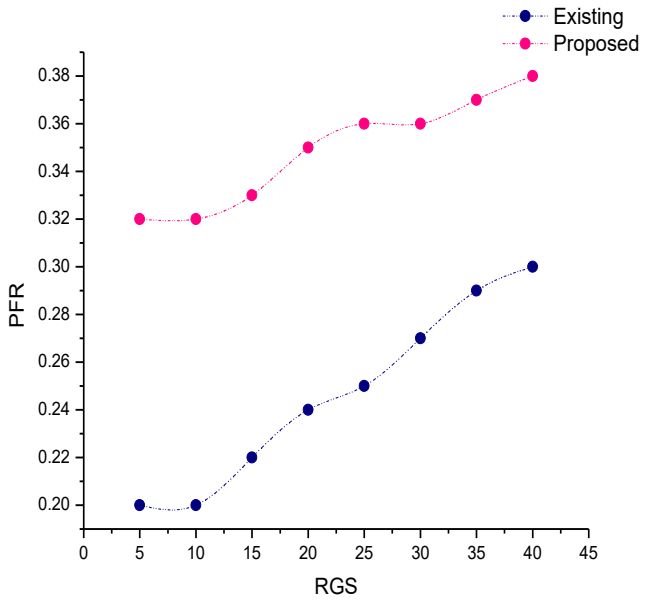

Figure 7 PFR – RGS

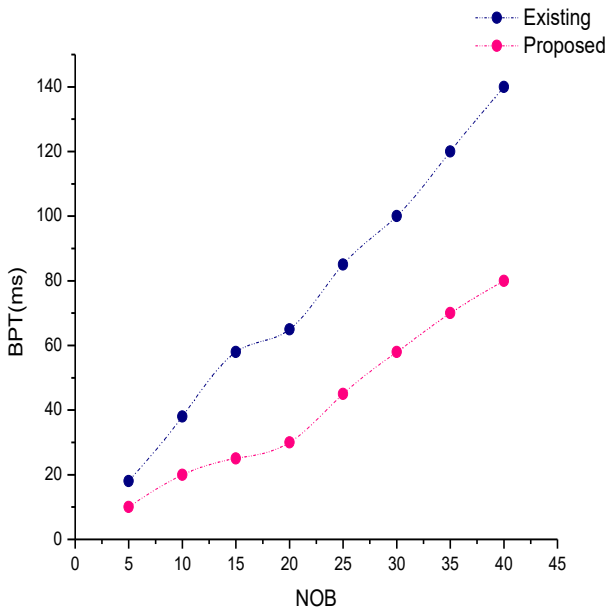

Figure 8 BPT – NOB

Figure 7 illustrates the impact of PFR on request generation speed; for evaluation, the packages generated contain 50% fraud packages and the remaining real packages. Our system was able to capture 38% of fraud packages out of 50%, and for the implementation where such a filtering module is not used, 30% of fraud packages are detected out of 50%. Also, in Figure 8, the time is taken to validate blocks before transferring. The proposed system uses both SDN and PFM for processing blocks before transferring, and it takes less time compared to the one in which only SDN is used.

5. CONCLUSION

This paper highlights the potential of SDN to revolutionize the way VANETs operate, providing centralized control and real-time adaptability, which are critical in dynamic vehicular settings. By integrating a package filtering model, these papers have illustrated the capacity to manage and optimize data traffic, thus improving network performance, security, and quality of service. This research contributes to the ongoing efforts to advance intelligent transportation systems, laying the foundation for more effective vehicular communication networks. The demonstrated benefits of the proposed approach underscore the potential for safer and smarter transportation systems, aligning with the evolving needs of our modern, connected world. In conclusion, the proposed work offers valuable insights into the realm of 5G-VANETs, showcasing the potential for SDN-based package filtering to foster enhanced networking and communication in vehicular environments. The primary objective of this work is to reduce the load on SDN, especially in terms of leverage due to fraudulent transactions and fraud packages. The proposed package filtering model (PFM) is a machine learning model trained using a logistic regression algorithm. The package filtering model is a classification algorithm used to classify packages into fraudulent or non-fraudulent. As the information and the transaction being carried out in this type of network are crucial, trust in terms of peers and the information being shared should be considered. Natural phenomena and other parameters (like testing the network with a controlled DDoS attack to test the package filtering model) are also considered while testing the system. In future the implementation of Zero Trust security principles in packet filtering can be done, by assuming that no entity, whether inside or outside the network, can be trusted, and focusing on strict access controls and identity verification.

REFERENCES

[1] Dharanyadevi, P., Therese, M. J., &Venkatalakshmi, K. (2021). Internet of Things Based Service Discovery for the 5G-VANET Milieu. In Cloud and IoT Based Vehicular Ad Hoc Networks (pp. 31–45). Wiley. https://doi.org/10.1002/9781119761846.ch2.

[2] Ahmed, A. A., Malebary, S. J., Ali, W., &Barukab, O. M. (2023). Smart Traffic Shaping Based on Distributed Reinforcement Learning for Multimedia Streaming over 5G-VANET Communication Technology. Mathematics, 11(3).

[3] Therese, M. J., Dharanyadevi, P., & Harshithaa, K. (2021). Integrating IoT and Cloud Computing for Wireless Sensor Network Applications. In Cloud and IoT-Based Vehicular Ad Hoc Networks (pp. 125–143). Wiley. https://doi.org/10.1002/9781119761846.ch7

[4] Luo, G., Zhou, H., Cheng, N., Yuan, Q., Li, J., Yang, F., & Shen, X. (2021). Software-Defined Cooperative Data Sharing in Edge Computing Assisted 5G-VANET. IEEE Transactions on Mobile Computing, 20(3), 1212–1229.

RESEARCH ARTICLE

[5] Hussain, Rasheed & Hussain, Fatima &Zeadally, Sherali. (2019). Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems. 101. 10.1016/j.future.2019.07.006.
[6] J. E. Naranjo, J. G. Zato, L. Redondo, M. Oliva, F. Jiménez and N. Gómez, "Evaluation of V2V and V2I mesh prototypes based on a wireless sensor network," 2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC), Washington, DC, 2011, pp. 2080-2085, 2011.
[7] Kawser, Mohammad & Sajjad, Syed & Fahad, Saymon & Ahmed, Sakib & Rafi, Hasib. (2019). The Perspective of Vehicle-to-Everything (V2X) Communication towards 5G. 19. 146-155.
[8] Xie, L., Ding, Y., Yang, H., & Wang, X. (2019). Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs. IEEE Access, 7, 56656–56666. https://doi.org/10.1109/ACCESS.2019.2913682.
[9] Qi, W., Song, Q., Wang, X., Guo, L., & Ning, Z. (2018). SDN-Enabled Social-Aware Clustering in 5G-VANET Systems. IEEE Access, 6, 28213–28224. https://doi.org/10.1109/ACCESS.2018.2837870.
[10] Abbas, M.T., Muhammad, A. & Song, W. SD-IoV: SDN enabled routing for internet of vehicles in road-aware approach. J Ambient Intell Human Comput 11, 1265–1280, 2020.
[11] Hakiri, Akram & Gokhale, Aniruddha & Berthou, Pascal & Schmidt, Douglas &Gayraud, Thierry. (2014). Software-Defined Networking: Challenges and research opportunities for Future Internet. Computer Networks. 75. 10.1016.
[12] Ali, Ali & Darwish, Saad & Guirguis, Shawkat. (2015). An Approach for Improving Performance of a Packet Filtering Firewall Based on Fuzzy Petri Net. Journal of Advances in Computer Networks. 3. 67-74. 10.7763/JACN.2015.V3.144.
[13] Dharanyadevi, P &Venkatalakshmi, K 2015, 'Potent Gateway Selection Algorithm for Integrated 3G-VMesh Milieu', World Applied Sciences Journal, ISSN: 1818-4952, vol. 33, no. 7, pp. 1228-1233.
[14] P. Dharanyadevi and K. Venkatalakshmi, 2016, Proficient routing by adroit algorithm in 5G-Cloud-VMesh network, EURASIP Journal on Wireless Communications and Networking, 2016:89, PP:1-11.
[15] S. Indriyanto, M. N. D. Satria, A. R. Sulaeman, R. Hakimi and E. Mulyana, "Performance analysis of VANET simulation on software defined network," 2017 3rd International Conference on Wireless and Telematics (ICWT), Palembang, pp. 81-85, 2017.
[16] M. A. Salahuddin, A. Al-Fuqaha and M. Guizani, "Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles," in IEEE Internet of Things Journal, vol. 2, no. 2, pp. 133-144, April 2015.
[17] Oliveira, Rogerio & Schweitzer, Christiane & Shinoda, Ailton & Prete, Ligia. (2014). Using Mininet for emulation and prototyping Software-Defined Networks. 2014 IEEE Colombian Conference on Communications and Computing, COLCOM 2014 - Conference Proceedings. 1-6. 10.1109/ColComCon.2014.6860404.
[18] X. Ge, H. Cheng, M. Guizani and T. Han, "5G wireless backhaul networks: challenges and research advances," in IEEE Network, vol. 28, no. 6, pp. 6-11, Nov.-Dec. 2014, doi: 10.1109/MNET.2014.6963798.
[19] Maniraj, S & Saini, Aditya & Ahmed, Shadab & Sarkar, Swarna. (2019). Credit Card Fraud Detection using Machine Learning and Data Science. International Journal of Engineering Research and. 08. 10.17577/IJERTV8IS090031.
[20] Ye, Jin & Cheng, Xiangyang& Zhu, Jian & Feng, Luting & Song, Ling. (2018). A DDoS Attack Detection Method Based on SVM in Software Defined Network. Security and Communication Networks. 2018. 1-8. 10.1155/2018/9804061.
[21] P. Dharanyadevi, Rajakumari &Venkatalakshmi K, "Qualitative Analysis on Ad hoc Routing Protocols", Middle-East Journal of Scientific Research, vol. 24, no. 4, pp.1194-1206, 2016.
[22] Tao, H., Zain, J. M., Band, S. B., Sundaravadivazhagan, B., Mohamed, A., Marhoon, H. A., … Young, P. (2022). SDN-assisted technique for traffic control and information execution in vehicular ad hoc networks. Computers and Electrical Engineering, 102.
[23] I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro, and E. Cerqueira, "Towards software-defined vanet: Architecture and services," in 2014 13th annual Mediterranean ad hoc networking workshop (MED-HOCNET). IEEE, 2014, pp. 103–110.
[24] K. L. K. Sudheera, M. Ma, and P. H. J. Chong, "Link stability based optimized routing framework for software defined vehicular networks," IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2934–2945, 2019.
[25] C.-M. Huang, M.-S. Chiang, D.-T. Dao, H.-M. Pai, S. Xu, and H. Zhou, "Vehicle-to-infrastructure (v2i) offloading from cellular network to 802.11 p wi-fi network based on the software-defined network (sdn) architecture," Vehicular Communications, vol. 9, pp. 288–300, 2017.
[26] B. Dong, W. Wu, Z. Yang, and J. Li, "Software defined networking based on-demand routing protocol in vehicle ad hoc networks," in 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN). IEEE, 2016, pp. 207–213.
[27] A. A. Khan, M. Abolhasan, and W. Ni, "5g next generation vanets using sdn and fog computing framework," in 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2018, pp. 1–6.
[28] Peng, Joanne & Lee, Kuk & Ingersoll, Gary. (2002). An Introduction to Logistic Regression Analysis and Reporting. Journal of Educational Research - J EDUC RES. 96. 3-14. 10.1080/00220670209598786.
[29] Sehrawat, P., & Chawla, M. (2023). Performance Evaluation of Machine Learning Algorithms applied in SD-VANET for Efficient Transmission of Multimedia Information. Multimedia Tools and Applications, 82(29), 45317–45344. https://doi.org/10.1007/s11042-023-15244-w.
[30] Mahaalakshmi, B., Padmapriya, R., Ellora Jeya Suji, J., & Cloudin, S. (2023). Smart Vehicle Health Monitoring System Based On ARIMA and Ordinal Logistic Regression for Analysis of Vehicle Parameters. In 2023 International Conference on System, Computation, Automation and Networking, ICSCAN 2023. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICSCAN58655.2023.10395495.
[31] Tripepi, G., Jager, K. J., Dekker, F. W., & Zoccali, C. (2008). Linear and logistic regression analysis. Kidney International, 73(7), 806–810. https://doi.org/10.1038/sj.ki.5002787.

Authors

Dr. P. Dharanyadevi holds a PhD in the faculty of Information and Communication Engineering from Anna University and M. Tech. in Computer Science and Engineering from Pondicherry University. She has a rich teaching and research experience in technical Universities of high repute. She has 35+ publications, in peer reviewed international journals and conferences with high impact factor and has authored 12+ book chapters. She is an active researcher in the field of VANET, internet of things, machine learning and web services. She is also an editor & reviewer of reputed International Journals. Dr. P.Dharanyadevi is a member of IAENG and ISTE.

Dr. Amirthasaravanan Arivunambi received the Ph.D. degree from Anna University, Chennai, Tamil Nadu, India, in 2017. He holds a B.Tech. degree in Computer Science and Engineering and an M.Tech. degree with a specialization in Information Security. With 15 years of teaching experience, he is currently serving as a Guest Faculty in the Department of Computer Science at Pondicherry University, Puducherry, India. His research interests include Information Security, Cloud Computing, System Optimization, Machine Learning, and the Internet of Things (IoT).

RESEARCH ARTICLE

B. Senthilnayaki has completed MTech and PhD at college of engineering Guindy, Anna University, and Chennai, India. She has 14 years of teaching experience. Currently, she is Associate Professor of the Department of Information Technology at St. Josephs Institute of Technology, OMR, Chennai India. She has more than 35 publications in reputed journals and conference proceedings. Her areas of interest include Machine Learning, Artificial Intelligent and soft computing.

Pethuru Raj, PhD is a chief architect at the Edge AI division of Reliance Jio Platforms Ltd. (JPL) Bangalore. Previously. Worked in IBM Global Cloud Centre of Excellence (CoE), Wipro consulting services (WCS), and Robert Bosch Corporate Research (CR). He had gained over 24 years of IT industry experience and nine years of research experience. He has finished the CSIR-sponsored PhD at Anna University, Chennai. He continued with the UGC-sponsored postdoctoral research in the Department of Computer Science and Automation, Indian Institute of Science (IISc), Bangalore. After that, he got two international research fellowships (JSPS and JST) to work as a research scientist for 3.5 years in two leading Japanese universities. He focuses on some of the emerging technologies, such as Artificial Intelligence (AI), Model Optimization Techniques, the Internet of Things Use Cases, Cloud-native and Edge Computing Paradigms, Reliability Engineering Practices, 6G Communication and Blockchain Technologies, Quantum Cryptography Algorithms, and Multimodal Generative AI Methods.

How to cite this article:

P. Dharanyadevi, Amirthasaravanan Arivunambi, B. Senthilnayaki, Pethuru Raj, “Enhancing 5G-VANET Environments with SDN-Based Package Filtering for Improved Networking”, International Journal of Computer Networks and Applications (IJCNA), 12(1), PP: 16-26, 2025, DOI: 10.22247/ijcna/2025/02.