International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.174

Intelligent Power Optimization Techniques for V2V Communication in IoT-Enabled Vehicles

AbidYahya
Department of Electrical, Computer & Telecommunications Engineering
Botswana International University of Science and Technology
Palapye, Botswana
yahyabid@gmail.com

Vishnu Kumar Kaliappan
Department of Computer Science Engineering
KPR Institute of Engineering and Technology
Coimbatore, India
vishnudms@gmail.com

Ravi Samikannu
Department of Electrical, Computer & Telecommunications Engineering
Botswana International University of Science and Technology
Palapye, Botswana
ravis@biust.ac.bw

Padmapriya[4]
Managing Director
Melange Publications
Puducherry, India
padmapriyaa85@pec.edu

S. Ganesh Kumar
Professor, Department of Data Science and Business Systems, School of Computing
SRM Institute of Science & Technology
Kattankulathur– 603203
ganeshk1@srmist.edu.in

Abstract—The Internet of Things (IoT) is utilized by an intelligent transportation application to arrive at informed conclusions for the benefit of passengers. The key advantages brought about by the Internet of Vehicles have been an improvement in both the quality of the driving and riding experience and an increase in both the safety and efficiency of traffic (IoV). The characteristics of distributed processing that mobile cloud computing possesses make it possible to process local data quickly. Internet-to-vehicle (IoV) connection may become more effective with the help of the vehicle cloud. This study centers on the communication between the vehicle and the other vehicle, as well as between the vehicle and the device on the road when necessary. The brief signature method of the authentication protocol was suggested, and it was discovered that it is not susceptible to forgery while employing a fresh scenario as the testing ground. We are developing a system and management methodology for IoV mutual authentication that is quick and effective. The suggested system was subjected to quantitative performance evaluation, which revealed that it is superior to other already existing systems in terms of its ability to interact with automobiles (vehicle-to-vehicle communication) and roadside equipment. The results are encouraging because there were relatively few instances of packet loss.

On the other hand, the scenario proposed in this paper aims to reduce the amount of power consumed by the devices installed in vehicles. This will be accomplished by efficiently controlling the transmission of information, making it so that the transmission power is proportional to the distance that separates one vehicle from another rather than transmitting at the highest possible power. The scenario was created by modeling the Matlab program using version 2021 of the software.

Keywords—intelligent, networks, Internet of Things, VANETs, IoT, IoV, V2V, V2Rt ,CLSS, Vehicles, mobile cloud.

I. INTRODUCTION

More and more industries are adopting the Internet of Things (IoT), including smart transportation and the nation's power grid. The Internet of Things (IoT) has been dominated by vehicles. Ad hoc networks are becoming increasingly widespread in vehicles (VANETs). Because VANETs can receive, evaluate, and interpret data from vehicles and structures throughout the globe, they cannot make intelligent decisions[1]. In contrast to VANETs, the Internet of Things (IoT) integrates cars, people, things, and networks into a single intelligent unit via networks such as deep learning, fog computing, cloud computing, and other technologies. IoV models at three, four, and five levels have been offered by authors who are experts in their fields. CISCO presented the four-level method, shown in Fig. 1, back in 2013. Personal devices, roadside units, and sensors account for most of this. Figure 2 displays several Internet of Things communication scenarios: The V2V (Vehicle-to-Vehicle) and V2Rt (Vehicle-to-Remote) protocols are used. IoV utilizes real information transmission between vehicles and everything (V2X) using wireless communication devices based on fog/edge computer technology. It has been considered an application of Cyber-physical systems (CPS). Different ways that V2X devices can talk to each other and how they connect are also talked about

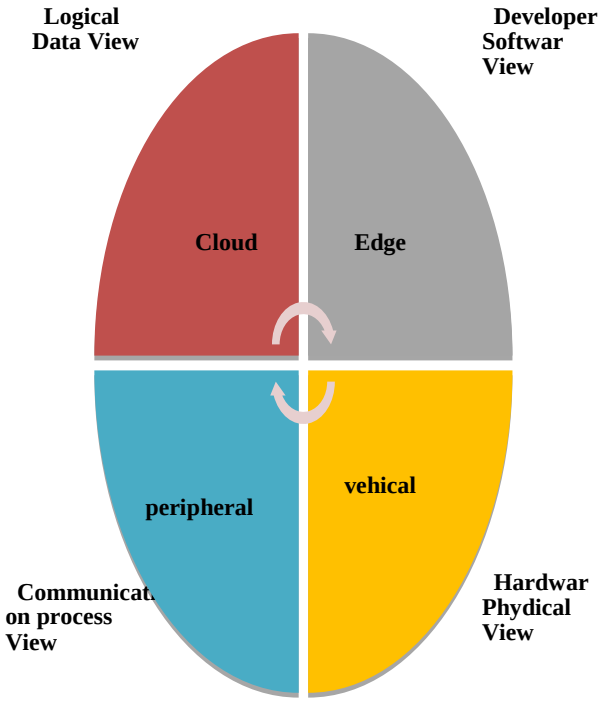

Fig. 1. IoV system model with four levels

DOI: rp-9788770040723.174

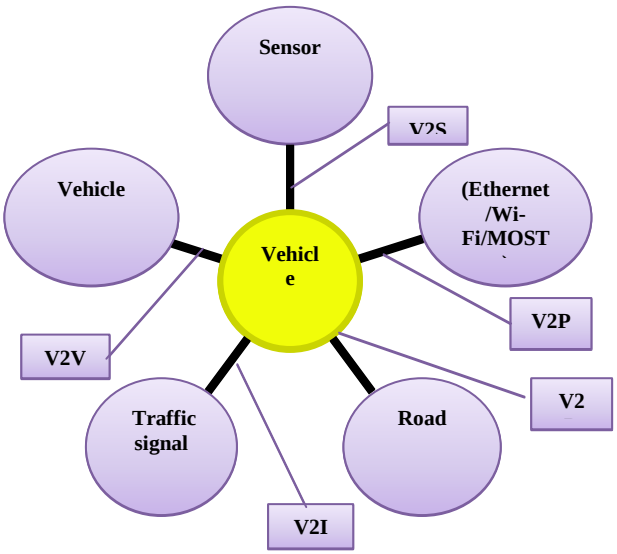

Fig. 2. IoV's multiple communications scenarios

Fig. 3. Illustration of an IoV Scenario

Integrating narrowband Internet-of-Things technologies improves vehicular communication systems' robustness, thereby enhancing service quality. This enhancement is achieved through two components that address latency and harmonic issues and a distributed antenna configuration for moving vehicles using machine learning and the across-entropy algorithm.

The proposed approach has been simulated and compared against state-of-the-art methods, demonstrating superior performance based on three key metrics: latency, mean squared error rate, and transmitted signal block error rate. The results indicate the proposed technique reduces peak power deficiency by nearly 49% at a probability of 10−3, yielding an additional 23.5% improvement through self-interference cancellation and a 31% decrease in bit error rate compared to existing literature. (Hamarsheh, Daoud, Baniyounis, &Damati, 2023)

It is possible to communicate between vehicles and network nodes (V2R), as well as between vehicles and personal devices (V2P) (V2S). The Internet of Things may benefit from a new hybrid communication paradigm that combines the advantages of both wired and wireless networks. Connecting automobiles to the Internet of Things improve their services' reliability and security. It is currently being developed for mobile devices to use mobile cloud computing (MCC), a kind of cloud computing. In [3], Vehicle cloud computing mobile vehicular cloud computing is a novel computing paradigm developed by Gerla based on the MCC architecture. Three resources are often found on vehicles and remote sensing devices: *data storage, sensors, and processing*. When these resources are linked to the Internet, a "vehicular cloud" is created, which may provide smart services. For example, a cloud server housed by a vehicle manufacturer may collect data about emergency road accidents and send it to a cloud service provider. It then informs the appropriate vehicles to pay attention to any newly uncovered information. The vehicle may upload data to the Internet anytime, anywhere. However, reducing the time spent on event processing will still be beneficial. Cloud computing and big data analysis work together in the Internet of Vehicles (IoV), making it even more intelligent since the IoV utilizes all of these technologies.

There have been several previous publications [3-6] to develop the technological infrastructure necessary for the Internet of Things. However, the Internet of Things continues to experience several difficulties.[7-11].

In the Internet of Things, security risks and privacy issues have become more relevant. When an attacker pretends to be a vehicle to transmit fraudulent signals, it can potentially disrupt the traffic patterns of other vehicles on the road. Several research on the security of IoV [12-14] have lately been brought to our attention. Protecting one's personal information is important for various reasons, including security. It is necessary to prevent unauthorized users from accessing a user's private information, such as their true identity location information. Even though each compromised car should be tracked down by an authorized government department using appropriate data and technology, this should be done accordingly[2]. In 2004, Huang et al. developed the certificate-less short verification approach and security model[15]. Xiang, et al. in [16] A revised, more effective strategy was also presented in 2022. Designers are concerned with securing access to private information through the Internet of Things (IoT). Considering the above issues and limitations, we suggest an effective anonymous authentication mechanism for the Internet of Things. The following is a summary of the most important contributions made by the paper:

- The suggested technique allows for conditional anonymous mutual authentication while protecting users' privacy.
- The introduction of a global methodology for vehicles is made. Vehicle verification may be performed in conjunction with RSUs in the same area.
- When compared to earlier techniques, our scheme has a lower computational cost.

The majority of this article is structured as follows. Section II overviews the IoV scenario model and some preliminary results. Afterwards, it is recommended that use

DOI: rp-9788770040723.174
a certificate with less short signature (CLSS). Using CLSS as a foundation, For the Internet of Things, Section IV introduces an unnamed access code Section V has both a security and a performance evaluation. Finally, Section VI finishes this paper.

II. PRELIMINARIES

Furthermore, we provide a scenario model for the Internet of Things, security protocols, and desired outcomes.

A. Scenario Model Design

The Internet of Things (IoT) scenario is shown in Fig. 3. TCC, TBA, vehicles, and RSU comprise most of the organization. A TCC handles everything from system initialization to data collecting from RSU, monitoring malicious vehicles, and updating the revocation list (Transportation Control Center). The RSU (Remote Sensor Unit) gathers and analyzes data from RSU, monitors hostile cars, and maintains the revocation list.

The TBA (Trace Back Authority) of a corrupt vehicle's function is to gather crucial information, verify harmful behavior, and impose sanctions as necessary.

Transport system: Every vehicle in the IoV has a built-in OBU that can wireless transmit vital highway safety information in real-time to other vehicles and RSUs.

Aside from that, it can receive and report data messages from other OBUs via a multi-hop mechanism.

Fixed route constructions (Roadside Units): RSUs are fixed route constructions erected along the side of the road. RSUs are normally connected to the TCC using a hardwired connection. They are in charge of capturing, transferring, and spreading real-time incoming communications from various sources. RSUs may act as access points for OBUs and offer them wireless services since they can handle messages within their respective ranges.

B. Model of Security

Constructing a CLSS involves the extraction of the private key, as well as the extraction of a secret value. Depending on the expert key's ability level, two groups will likely have attempted to break into CLSS. The AI would replace every user's public key even without passcodes. AI may access the parent vital but cannot modify any user's public key until specific conditions are met. Our approach will be irreversible in the presence of uncertainties compared to modified chosen message and ID assaults in inconsistencies in the Two attracter. Because the nodes (vehicles) in VANETs are supplied with considerable power sources, they have an advantage over regular ad hoc networks. Using VANETs, cars may interact with one another and with roadside infrastructure (V2I), allowing drivers to be more aware of their surroundings and improving safety while potentially streamlining traffic flow. The programs that operate on VANETs may be roughly divided as follows:

- Safety-related apps - for example, Emergency Messages
- Business-related applications
- Best-effort applications, such as infotainment systems
- secure Transactions, such as toll collecting

The vast majority of crucial communications To be successful, safety warnings broadcast through VANETs must go deep into the network and be sent quickly. This communication must be secure, and no personally identifiable or linkable information should be disclosed to other parties due to the legal right of vehicle owners participating in it to remain private. In this instance, VANET security is most important. Authentication is crucial in Vehicular networks since there may be both harmful and legal sources of communication. Authentication refers to the ability to distinguish between multiple sources.

For a communication to be considered anonymous, the physical identity of the sender should not be deducted from the message.

• *Data Integrity* - The authorized party's data has not been altered in any way and is received precisely as it was. The IEEE 1609 standards define Wireless Access in Vehicular Environments (WAVE) communication protocols for vehicular networks. IEEE P1609.2 specifies that [2] Private messaging protocols In this topic, the DSRC's layouts, and techniques for processing encrypted messages are discussed and standardized [3] to implement an encryption system that takes advantage of PKI (PKI). Additionally, the administrative operations necessary to provide important security services, such as canceling a vehicle's certificate after it has been given, are detailed in this paper.

III. AN OVERVIEW OF PKI FROM THE PERSPECTIVE OF VANETS

The public key infrastructure relies on asymmetric key cryptography as its base. In a PKI system, each principal's keys are assigned: Keys (Private and Public Key). Unlike the private key, the public key may be shared with any of the network's other participants. Pr(.) and Pu(.) are two functions that represent the private and public keys, respectively; each function has the property of being an individual.

$$M=Pr(Pu(M))$$

$$M=Pu(Pr(M))$$

The message M provides here is how the keys are meant to guard against.

Messages are signed with a private key, and an attachment is attached to the message to secure the integrity of the message's transmission throughout transmission. When the receiver receives this message, they may use the public key of the (sender) to verify that the message has been signed. This solution has a basic flaw: swapping keys without compromising their integrity is impossible. Trusted nodes [4], known as Certificate Authorities, are one generally acknowledged solution for this problem (CA). Certificates, which assist in establishing the link between the owner of the private keys and the owner of the corresponding public keys, are used to validate data as part of this method.

To be more specific, an (unsigned) certificate must have the following parts in compliance with IEEE 1609.2:

DOI: rp-9788770040723.174

1) The public key
2) The certificate's expiration date and time
3) This list of CRLs relates to the certificate at issue. Everything described above is included in the certificate that the CA. will issue in addition to the CA's seal. Because there will only be one CA in the whole network, each PKI system entity must have access to the CA's public key. To ensure that only CA-verified certificates may be trusted. The IEEE 1609.2 Standard mandates that a verified message must include the sender's certificate, the public key used to sign the message, and the message itself since all of a CA's certificates must be distributed.

CA certificates may also be cancelled for several reasons not covered in this article. [6] The assailant's certificate may be temporarily cancelled until a connection with the CA can be established in a concept for certificate cancellation in-vehicle networks. Certificate revocation lists (CRLs) are used to send information on a certificate's revocation, including but not limited to the data stated below.

1- The following is the CRL series number: The sequence of CRLs intended by this CRL All revoked certificates are listed under
2- "Entries."A message's verification cost includes checking whether or not certificates in CRLs are present and usable at this period. Consequently, timely access to this revocation information is essential to the overall robustness and dependability of the operation. Providing real-time CRLs in car networks is a challenging problem to address.

IV. Developing The Cos for fheVanet Using Analytical Methods

There are a few permanent spots in the area that we're interested in where cars may use information-fueling stations on an as-needed basis (the duration between visits is random, with an average of several days). Information-fueling stations provide the latest current CRLs to the automobiles that stop there. This example shows how to compute a system's CoS and the various system factors that influence it.

Some mobility model is considered, and each vehicle has a certificate used to verify the authenticity of communications in this system. To count the number of other vehicles that have sent messages to a tagged vehicle in the future, examine a vehicle and define the c(t)t0 counting method (t). V2V communication between vehicles is boosted due to the tagged vehicle's higher contact rate with other vehicles.

Considering that, the limit exists nearly without a doubt. The process c(t)≥t0 is a random process.

$$\lambda = \lim_{s \to \infty} \frac{c(t)}{t}$$

Using r(t)tt0 to count the number of certificates that have been cancelled at any set moment and then using

$$r = \lim_{t \to \infty} \frac{r(t)}{t}$$

Because we're just interested in the average behavior of multiple automobiles, we'll assume that the process "c(t)" isn't significantly influenced by (or related to) the process "r(t)." Consider the potential of a coupling between c(t) and r while considering a small number of cars (t).

The CRLs of the tagged vehicle are updated in line with a method independent of the CA (either via RSUs or info-fueling stations). The identified car performs m(t)0 CRL updates. An independent and identically distributed random sequence of random variables will be utilized to estimate inter-update intervals (the time between subsequent CRL updates).

(Hamarsheh et al.)i≥1. E[T] = E[Ti] and E[T_2] = E[T_2 I then. The CRL of the tagged vehicle is presumed to be updated at time 0 since we are primarily concerned with system time average behavior (the CoS). Counting processes under examination are assumed to have limited second moment intertransition periods.

The processes 'c(t)' and 'r(t)' are expected to vary at a faster time scale than the process'm(t), i.e., the time scales of the processes 'c(t)' and 'r(t)' are shorter than the time scales of the process'm(t)' ⌊ E[T] and r E[T]. It is reasonable to assume that m(t) processes observe an averaged out representation of both procedures, given that the second moments of intertransition instants are limited. These counting procedures are thought to have constrained second-moment intertransition periods.

C(t) and r(t) are expected to vary at a quicker time scale than the'm(t)' process, which is defined as the time scale of E[T]. An averaged out picture of either method is what the m(t) process sees since the second moments of intertransition times are limited.

V. Positioning of Car

To continue data dissemination in VANETs, the suggested protocol needs a suitable categorization of neighboring vehicles. First, the number of receiving cars inside the transmission zone is determined by combining data from nearby vehicles with that obtained during the data collection phase. It then separates its transmission area into many segments, each representing a distinct area, as indicated in Fig. 4 (the source vehicle).

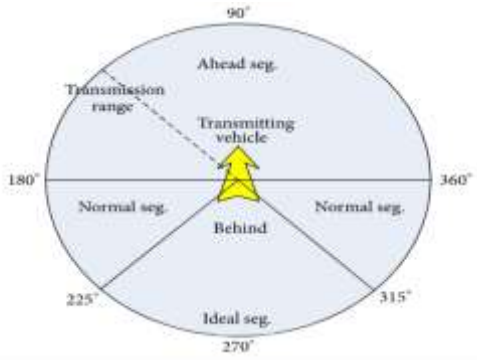

Fig. 4 Transmission range divided into segments

DOI: rp-9788770040723.174

Each receiving vehicle (denoted by) is categorized into three groups: ideal, normal, and ahead cars, once the segmentation process has been finished. As a result, the data packet's next forwarder should be one of the furthest cars in the optimum segment travelling toward the source vehicle. One vehicle at the far end of the ideal segment must retransmit a data packet with the lowest possible latency and eliminate the need for multiple retransmissions. A data packet will be sent to whichever vehicle is furthest from the optimum section if there isn't a vehicle. In the same way, if no vehicles exist inside the ideal or normal segments, the data packet will be sent to the vehicle(s) furthest from the forward segment. Data packets are intended to be sent to as many nearby cars as possible that aren't immediately accessible to the source vehicle by vehicles located inside the high-priority segments. Algorithm 1 explains how to determine whether the receiving vehicle is in the wagon wheel's ideal, normal, or forward section and how to proceed accordingly.

- ✔ Procedure for Choosing a Next Forwarder Vehicle (NFV)
- ✔ Procedure for Choosing a Next Forwarder Vehicle (NFV)
- ✔ Sourceβvehicle (S) that initiates the data dissemination process
- ✔ (Tx, Ty)β x and y coordinates of transmitter vehicle (Tj) on 2nd and subsequent hops
- ✔ (Rx, Ry)β x and y the location of the vehicle that will receive the message (Ri)
- ✔ Outputβ NFV/number of cars to distribute data/number of vehicles to deliver data (s)
- ✔ Ifβit's the first time do
- ✔ Ifβ The Orientation Ri to for a certain threshold value of the Orientation Ri and Tj
- ✔ Position Ri toβatan2 (arctangent function)
- ✔ Distance Ri-Tj
- ✔ IfβRi is included inside the ideal segment, i.e. between angles 226° and 324°, thenset waiting time for priority 1
- ✔ otherwise 2
- ✔ end
- ✔ end
- ✔ else βset priority 3 waiting time ;
- ✔ end Ri. Otherwise 1,
- ✔ If βa message is already scheduled, cancel it and trash it.
- ✔ end
- ✔ Cancel planned message
- ✔ end

VI. Result and Conclusion

The suggested new protocol operates in various VANET traffic circumstances. Initially, we examined a 20-kilometre-long, three-lane highway with cars moving in the same direction. Vehicle flow production is constructed at each highway's opposing edge, producing and inserting vehicles at 30, 40 and 50, vehicles/hour. In this scenario, overtaking is performed by putting three categories of cars into the network: high, moderate, and slow-speed vehicles. Vehicles of these three categories may attain maximum speeds of 30, 22 and 26 meters/sec. An example of such a situation would be a dynamic vehicular network with three vehicle kinds. During the simulation, the speed of these vehicles varies. Each simulation comprises 40% high, 15% moderate, and 20% low-speed cars. When considering the first situation, it was taken into consideration that the cars are traveling in a straight line and at varying speeds. However, they are quite near to one another. In figure 5 demonstrates that the first vehicle, which is colored red, is only sending out information in the form of packets with a transmission diameter that is proportional to the distance between it and the car. This is done for two reasons: on the one hand, to reduce the amount of power that is being wasted, and on the other hand, to ensure that the information being sent out does not become distorted due to interference. The first car sent constant communications and information about the current state of the road to the second and third cars, which were colored black and yellow, respectively. This will result in a lower rate of lost packets and lower overall power consumption from the processor. It illustrates the ideal case for the proposed scenario, considering that there is no communication system free of packet loss., as demonstrated in the algorithm proposed in the paper.

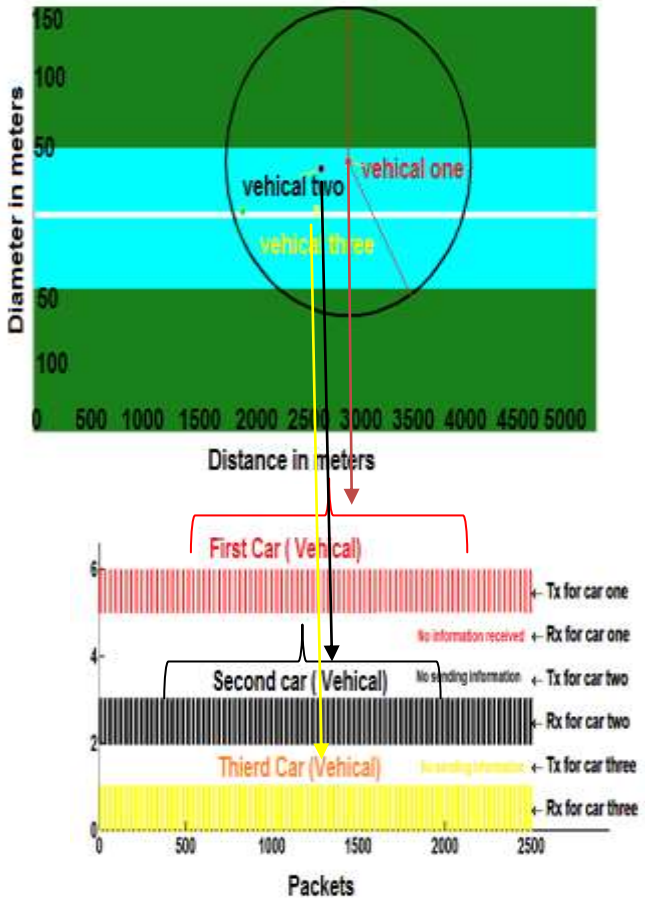

Fig. 5 vehicle transmission and received Data

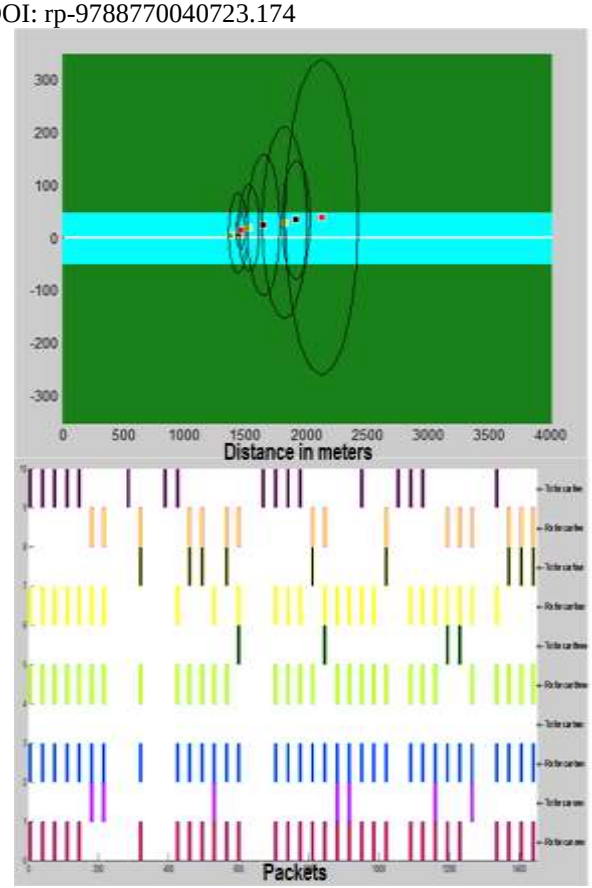

Fig. 6 illustrates the number of packets (Tx and Rx) for five vehicles.

The second scenario, depicted in Figure 6, involves more cars on the road than three, all moving at varying speeds. It should be noted that if any vehicle deviates from the prescribed diameter for broadcasting for the first vehicle, the vehicle closest to it will broadcast information with a diameter proportional to the distance it is from the car that came before it. The number of packets that were successfully received by each vehicle is depicted in Figure 6, together with the number of packets that were unsuccessfully received. The new protocol has a noticeably low packet loss figure 7, which reduces both the energy consumption of the transceiver system placed in the automobile and the consumption of the Internet package. As a result, the cost of both the Internet package and its delivery is reduced.

VII. Conclusion

The paper concludes by introducing a novel VANET protocol that performs well under various traffic conditions. The simulation results demonstrate that the proposed protocol reduces overall power consumption and packet loss, making it a financially viable solution. Given that no communication system is completely free of packet loss, the algorithm presented in the paper illustrates a perfect case for the suggested scenario. The two scenarios examined in the paper, where a high number of packets were successfully received by each vehicle, provide additional evidence of the protocol's effectiveness. Overall, the paper offers insightful information about creating effective VANET communication protocols, which can enhance the effectiveness and safety of vehicular networks.

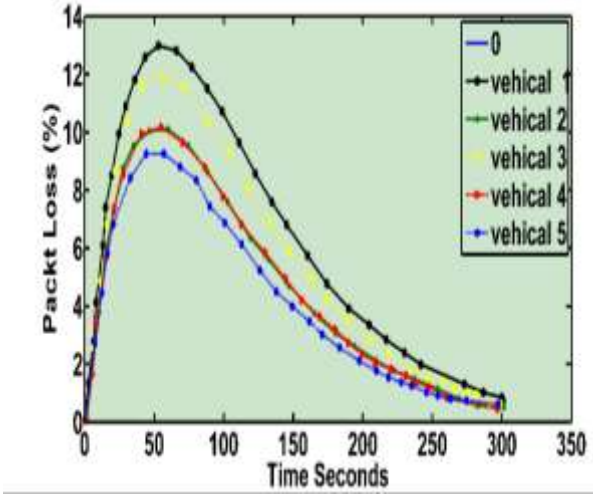

Fig. 7 illustrates the packet loss for five vehicles.

References

[1] M. Gillani, et al., "Data collection protocols for VANETs: a survey," Complex & Intelligent Systems, p. 1-30, 2022.

[2] K.A. Jani,and N. Chaubey, "IoT and Cyber Security: Introduction, Attacks, and Preventive Steps, in Quantum Cryptography and the Future of Cyber Security," IGI Global. p. 203-235, 2020.

[3] S.K. Panda, and S. Das, "An Energy-Aware Service Management Algorithm for Vehicular Cloud Computing, in Advances in Distributed Computing and Machine Learning," Springer. p. 22-33, 2022.

[4] X. Zhou, et al., "Information diffusion across cyber-physical-social systems in smart city: A survey,"Neurocomputing, vol. 444,pp. 203-213,2021.

[5] Rajesh, M., &Sitharthan, R. (2022). Introduction to the special section on cyber-physical system for autonomous process control in industry 5.0.Computers and Electrical Engineering, 104, 108481.

[6] X. Du, and F. Lin, "Maintaining differentiated coverage in heterogeneous sensor networks," EURASIP Journal on Wireless Communications and Networking, vol. 2005, no. 4, pp. 1-8, 2005.

[7] C. Wang, et al., "A survey: applications of blockchain in the Internet of Vehicles," EURASIP Journal on Wireless Communications and Networking, vol. 2021, no. 1, pp. 1-16, 2021.

[8] M.Srinivas, et al., "A Review Article on Wireless Sensor Networks in View of E-epidemic Models," Wireless Personal Communications, p. 1-17, 2021.

[9] S. Yu, et al., "Malware propagation in large-scale networks," IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 1, pp. 170-179, 2014.

[10] P.V. Suryanarayana,and K. Surendra, "Malware Propagation in Large-Scale Networks".

[11] H. Abualola, et al., "A V2V charging allocation protocol for electric vehicles in VANET," Vehicular Communications, vol. 33, p. 100427, 2022. Sitharthan, R., Vimal, S., Verma, A., Karthikeyan, M., Dhanabalan, S. S., Prabaharan, N., ...&Eswaran, T. (2023). Smart microgrid with the internet of things for adequate energy management and analysis.Computers and Electrical Engineering, 106, 108556.

[12] H.Y.Lin, Hsieh, M.Y.and Li. K.C., "A Fast Fault-Tolerant Routing with ECDSA Signature Protocol for Internet of Vehicles," In Proceedings of Sixth International Congress on Information and Communication Technology, Springer, 2022.

[13] J. Mahmood, et al., "Secure Message Transmission for V2V Based on Mutual Authentication for VANETs," Wireless Communications and Mobile Computing, 2021.

[14] D. Xiang, et al., "A secure and efficient certificateless signature scheme for Internet of Things," Ad Hoc Networks, vol. 124, p. 102702, 2022.

[15] E.F. Cahyadi, and M.S. Hwang, "A Comprehensive Survey on Certificateless Aggregate Signature in Vehicular Ad Hoc Networks," IETE Technical Review, p. 1-12, 2022/.