Privacy Preserving Data Transmission in Malicious Vehicular Adhoc Networks

Mrs.R.M.Rajeshwari[a], Dr.S.Rajesh[b]

[a]Assistant Professor,Research Scholar/Anna University,Tamilnadu,India
[b]Associate Professor/Mepco Schlenk Engineering College
Email:[a]rajimurugesan@gmail.com,[b]srajesh@mepcoeng.ac.in

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Vehicle Adhoc Network is deployed on the road, where vehicles constitute mobile nodes in which active security and intelligent transportation are important applications of VANET. VANETs are a key part of the intelligent transportation systems (ITS) framework. Sometimes, VANETs are referred as Intelligent Transportation Networks. However, authentication and privacy of users are still two vital issues in VANETs. In the traditional mode, the transactional data storage provides no distributed and decentralized security, so that the third party initiates the dishonest behaviors possibly. VANET has temporary participants , communication between vehicles are short-lived messages. Possible situation might happens , adversary may play as an legitimate user and able to perform malicious activity .To address these challenges this paper proposes timestamp based message between users to perform secure data transmission and give the negligible probability of the attacker. With the help of Certificate Authority (CA) and the RoadSide Units (RSUs), our proposal attains the confidentiality and trace the identity of the unauthenticated vehicle in the anonymous announcements as well. Finally, through the theoretical analysis and simulations, our scheme is able to implement a secure VANET framework with accountability and privacy preservation

Keywords: CA,RSU,MVD,OBC,ECC

1. Introduction

VANET typically consists of vehicles and properly distributed roadside units (RSUs)[4].A vehicle can send/receive safety-related messages (e.g., speed, location, dangerous road conditions) to/from nearby vehicles and RSUs.These messages reduce the drivers' risk of having an accident and help them manage small emergencies.It is essential to ensure that the safety-related messages are

- authenticated, confidential and unmodified.
- In VANETs, a vehicular message usually contains information on a vehicle's speed, location, direction, etc. From those messages, a lot of private information about the person can be inferred.
- A malicious vehicle could send fraudulent messages for its own profit or impersonate other vehicles to launch attacks without being caught
- In order to prevent this security issues ,we are in need to maintain the encryption, authentication and integrity of the message using Block Chain and ECC Privacy Preserving Authentication Mechanism

Suppose Previous vehicle met with an accident ,we get the alert message . To confirm that the message is correct or fake we need security mechanism.Consider a Scenario , VIP Smart car has inbuilt wireless enabled device such as (OBU) to communicate with their security guard Vehicle.Hacker may act as registered user and able to get the VIPs Vehicle identity to perform an Missle Attack[2] .In order to prevent that ,to hide the vehicle's identity as well as perform data transmission between the vehicle, tamper proof device was designed to avoid security breaches. We are taking this idea and changed our work based on network architecture and protocol functionality.OBC(On Board Chip) of the vehicle receive the message and respond accordingly between the vehicle.Vehicle are registered with CA(One Time),To avoid all types of attacks and any node containing fake/untrusted messages ,are blocked by Block Chain Concept integrated with ECC.If a node enter as register user, and Perform any malicious activity, his activity is compared with other relevant activities ,if anything suspicious, his registration is disabled and he will be blocked from communication chain.

2.Related Works

Zhu, Liehuang, et al. discussed thatthe location and identity of the vehicle is preserved for ensuring the privacy in VANET[6]. As the vehicles may undergo collision attacks, data privacy is considered as a critical phenomenon. The homomorphic encryption and data perturbation is adopted to enhance the security in unique features of the VANET. The homomorphic cryptographic technique ensures privacy of data, location and identity of vehicles, whereas the conventional Advanced Encryption Standard (AES) attains to identity privacy.

Cui, Jie, et al in his paper dealt with mutual authentication scheme for security is proposed to ensure that there is no fake message in the broadcasting zone. It also helps in preventing the side channel attack, in which the attacker requires identity and encryption key of the device. The mutual authentication eliminates the bilinear pairing, which in turn attains cost efficiency. The dynamic region topology algorithm is developed by integrating both symmetric and asymmetric cryptographic techniques, namely AES and Elliptic Curve Cryptography respectively. The social network in the corresponding zones is utilized to send the messages to the vehicles. In general, the symmetric key cryptography results in non-repudiation, whereas the asymmetric key cryptography results in computation and storage overhead. These issues are resolved by integrating both the symmetric and asymmetric techniques was reported byMichael Crosby.Shah, Syed Asad, et al discussed.

A distributed trust framework for VANETs which incorporate pseudonym concept to enable privacy module is described. The pseudonyms of the vehicles are changed periodically to preserve themselves from the trackers. The Reputation Label Certificate (RLC) which stores the reputation values in the central database helps in ensuring the trustworthy vehicles in the communication zone. The reputation updating algorithm updates the reputation values of the vehicles in the database based on their activity of broadcasting messages. These reputation values greatly help in attaining the security and privacy requirements.

2.1.Our Contribution

In VANET there is no permanent sender or receiver ,message forwarding between the vehicles are temporary so it does need to store the message , but authentication and time stamp concept is employed .For example consider there is an road damage ,it may be repaired with in 30 minutes, then that alert message is forwarded to the registered vehicles. After 30 minutes there is no use of forwarding the message so we need a time stamp to tell when it will be expired too. This concept was not discussed in previous work. Not only fake messages, the messages broadcasted by the real vehicles may also cause harm if the messages are delivered are not delivered on time. It is essential to maintain strict timestamp, thereby reducing the delay in the network. Thus we can avoid unnecessary message delivery and also save time and energy.

2.2.Proposed Time Stamp Based Security Model

The proposed system consists of a root trusted authority (CA), a number of RSUs and vehicles.Vehicle registration Confirmation at each time, checking vehicle is registered or not by third party is unsuccessful attempt that it will increase complexity as well as delay. For that initially we assume that all vehicles are registered to CA and get token from CA.When the vehicle enter in to a city traffic or toll gate or whenever it cross the toll gate ,it is automatically added to the Block of the corresponding region and hash key for the block in the particular region is generated.If Vehicle enters, it may add in to the communication chain,but any changes are made from the Block it will be reflected to others,Thus they can avoid unwanted message/fake message from registered User.This can be explained by the following scenario , For eg In BitCoin Application if 10 persons involving money transfer,holding 100 rupees each.If any one perform malicious activity,then corresponding hash for 100 Rupees data is reflected in all persons in the chain.So we automatically detect the malicious node and never establish block chain communication with him.Similar manner, we deal with malicious node activity which is the initial step of Block chain. In our Vehicular networks ,vehicles entered with in the particular toll(from starting point and ending point of the Toll Gate) are grouped together and Block.is created..Once the message forwarding is completed,Block is disabled,its Hash value are no longer maintained.But the identity of the vehicle remains in the network for future communication

Vehicle Registration Algorithm

- ***Step 1:*** Vehicle obtains real ID(Registration Number)from the Motor Vehicles Division (MVD), and communicates with CA to get Token .

- ***Step 2:*** CA verifies firstly the existence of real identity about registered vehicle,(one time) allow to participate in Vehicle communication by generating pair of ECC Public-Private keys namely Pki and Ski and Pseudonym ID according to real identity of vehicle;

- ***Step 3:*** OBU calculates two hash functions, which are H0 = (P IDi ||Pki) and H1 = (V IDi ||cert) in order to authenticate vehicle identity for future communication and create Block for the vehicle in particular region

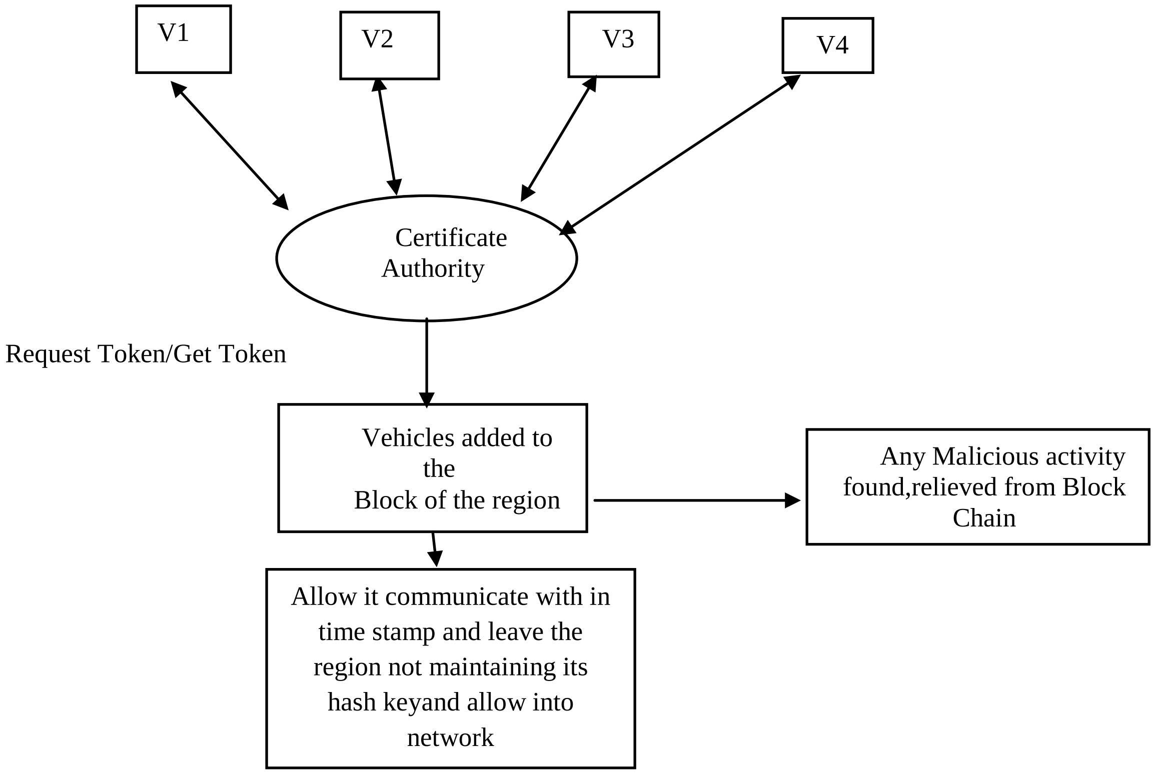
Certificate Validation and Revocation Algorithm

- ***Step 1:*** Once the vehicle enter in to network it communicate with RSU by its Pseudo ID and Public Key

- ***Step 2:*** OBU verifies it by comparing the hash value of Pseudo ID/Public Key pair with its real ID/private Key (one time) with CA and if it matches allowed to participate .Then Block chain for the particular region is allocated to the vehicle
- ***Step 3:*** After determining the authenticity of the vehicle identity, Block will be enable with in particular toll region .
- ***Step 4:***The RSU packs up a transaction T(sigSki (H1)||P IDi ||Pki)and stores the vehicle identity in the block-chain network by leaving Hash key value temporarily

Vehicle Advertisement Phase

- ***Step 1:*** The RSU monitors the traffic event(E) to form a new transaction whose content is Tx(E||P IDi||timestamp).
- ***Step 2:*** Each vehicle calculates the timestamp of alert message and validates the message expiration time
- ***Step 3:*** If the message has the validity to handle the emergency situation and matching required validation parameters such as direction and integrity proof which can be forwarded to next vehicle
- ***Step 4:*** Else message will be discarded in same time to avoid delay and save energy and time of RSU


V1
V2
V3
V4
Certificate Authority
Request Token/Get Token
Vehicles added to the Block of the region
Any Malicious activity found,relieved from Block Chain
Allow it communicate with in time stamp and leave the region not maintaining its hash keyand allow into network

The above figure shows the overflow of proposed model.

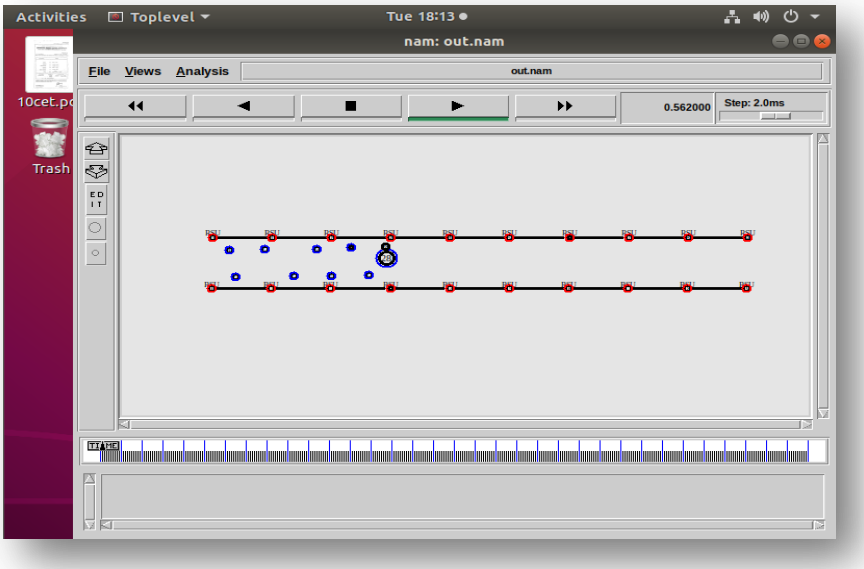
3.Results and Discussion

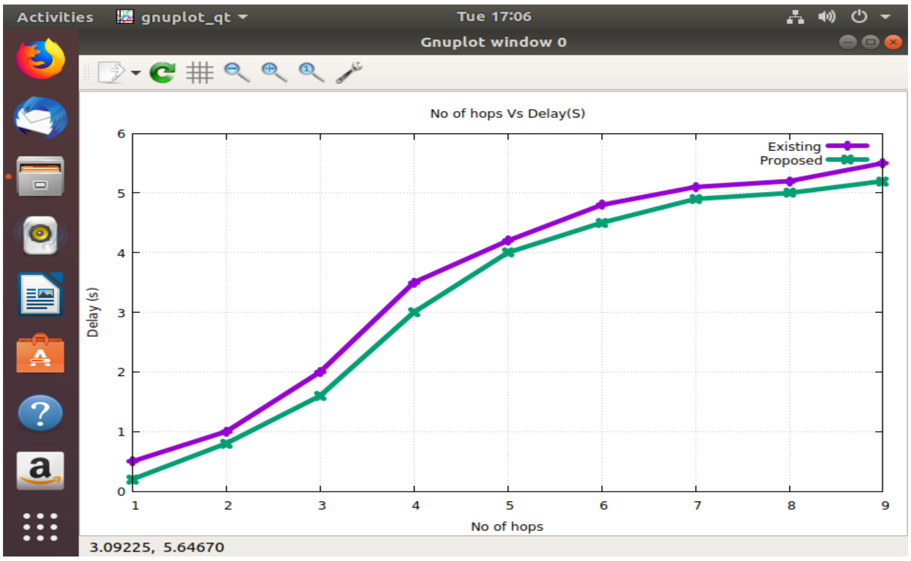
Performance analysis for the proposed model is studied for 20 vehicles using NS2 tool and the metrics like delay, packet delivery ratio and throughput are analyzed. The proposed Timestamp based Algorithm is compared with the existing algorithms.

End to end delay is defined as difference between the packet delivery time at destination and the packet origination time at source.

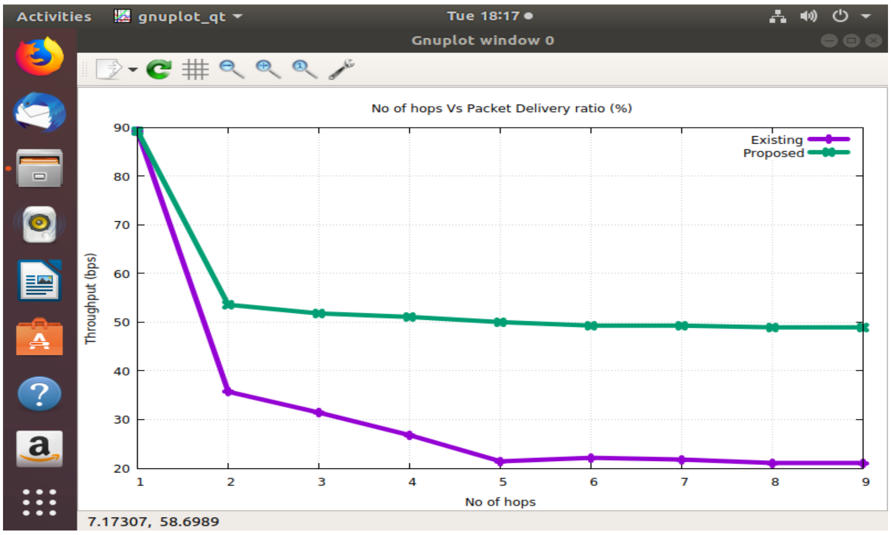
End to End Delay = Packet delivery time at destination – Packet origination time at source

Delay must be minimum in the network in order to have proper and correct time of packet reception in real time cases.





Packet delivery ratio is defined as the ratio of successful data packets received by destination to the data packets generated by the source. The verifiers in the network monitors the packets transmitted between the nodes. The packet delivery ratio of the proposed Monitoring Algorithm is much better when compared to the existing techniques. As the number of malicious nodes increases, packet delivery ratio of the network decreases. Throughput is defined as the ratio of total packets received to the difference between stop time and start time of the packets. As the active time of the network increases (for fixed set of nodes), the successful packet transmission rate also increases



4.Conclusion

Time Stamp Based Communication Algorithm is introduced in this paper to implement security parameters in VANET. Algorithm testing is more effective than the VSRP and CA algorithms that are used in the current process. Simulated tests indicate that the proposed algorithm would result in less delay and improved efficiency relative to traditional approaches in literature based on VANET..

References

[1]V S. Padmapriya, R. Valli, M. Jayekumar,” Monitoring Algorithm in Malicious Vehicular Adhoc Networks, IEEE ICSCAN2020

[2]Vasudha ,FahiemAltaf,SoumyadevMaity “Linearly Homomorphic Signature Based Secure Computation Outsourcing in Vehicular Adhoc Networks”, 2019 Innovations in Power and Advanced Computing Technology (i-PACT)

[3]Anil Kumar Sutrala , Palak Bagga , Ashok Kumar Das,” On the Design of Conditional Privacy PreservingBatch Verification-Based Authentication Scheme for Internet of Vehicles Deployment”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 69, NO. 5, MAY 2020

[4]Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang. ”AnIDbased linearly homomorphic signature scheme and its application in blockchain”. IEEE Access, 6, pp. 20632-20640.IEEE, 2018.

[5]J. Li, Y. Zhang, X. Chen, and Y. Xiang. ”Secure attribute-based data sharing for resource-limited users in cloud computing”. Computers & Security, 72, pp. 1-12. Elsevier, 2018.

[6]L. Zhang,, Q. Wu, B. Qin, J. Ferrer, and B. Liu. ”Practical secure and privacy-preserving scheme for value-added applications in VANETs”. Computer Communications, 71, pp. 50-60. Elsevier, 2015

[7]M. Zhang, C. Chen, T. Wo, T. Xie, M. Bhuiyan, and X. Lin. ”SafeDrive: online driving anomaly detection from large-scale vehicle data”. IEEE Transactions on Industrial Informatics, 13(4), pp. 2087-2096. IEEE, 2017.

[8]P. Li, J. Li, Z. Huang, C. Gao, W. Chen, and K. Chen. ”Privacypreserving outsourced classification in cloud computing”. Cluster Computing, 21(1), pp. 277-286. Springer, 2018.

First Author: Mrs R.M .Rajeshwari

Worked as Assistant Professor in Computer Science Engineering Department in reputed Engineering Colleges for 9 Years and Receiver of University Rank ,now Currently Pursuing Doctorial programme under Anna University Chennai. Completed B.E (CSE) at Mohamed Sathak Engineering College(2004) , M.Tech (Network Engg) at Kalasalingam University and Pursuing Ph.D in Anna University as Research Scholar.

Second Author: Dr.S. Rajesh

Working as Associate Professor in Information Technology Department in reputed Engineering Colleges for the past 19 Years. Area of interest in Image Processing. Journal Publications :33 international papers, International Conference: 24 and National Conference & Others: 4. Membership in ISTE, IETE & CSI.

Title of Ph.DThesis:Land Cover/Land Use Mapping Using Optimized Wavelet Packet Transform Features.