International Journal of Advanced Technology in Engineering and Science
Vol. No. 10, Issue No. 04, April 2022
www.ijates.com
ijates
ISSN 2348 - 7550

Traffic Management Using VANET And 5G

Gayatri Gaikwad,
Student , Computer Engineering, Trinity Academy of Engineering, Pune, India
gayatrisg29@gmail.com
Sanyukta Holkar,
Student , Computer Engineering, Trinity Academy of Engineering, Pune, India
sanyuktaholkar24@gmail.com
Dr. Nilesh Uke, Professor ,
Computer Engineering, Trinity Academy of Engineering, Pune, India
nilesh.uke@gmail.com

Abstract
The purpose of Vehicular Ad-hoc Network (VANET) cloud, is to provides several computational services to attenuate hold up, traveling time, accidents, traffic rule violation, and environmental pollution. Today car manufacturers have already began to equip vehicles with sophisticated sensors which will provide many assistive features like front collision avoidance, automatic lane tracking, partially autonomous driving, suggestive lane changing, and so on. Such technological advancements are enabling the adoption of VANETs not only to supply a safer and more well-off driving experience but also to supply many other useful services to the driving force in addition as passengers of a vehicle. The increasing number of on-road vehicles has become a serious cause for congestion, accidents and pollution. Collision avoidance using automatic braking and camera based surveillance are some other applications that we addressed. VANET faces threats in three different fields; security, safety, and infotainment, which further have numerous attacks. More precisely, this research conducted an in-depth study and proposed a VANET trust model which is integrated with the concept of 5G which plays a major role within the efficiency of network security and creating more and faster channels for communication .

VANET, 5G, trust model, ITS, VANET cloud, trust value, transient ticket, connected vehicles, IoT, traffic management, intelligent transportation

1. Introduction

The development of society and economic growth leads to a drastic increase in the number of vehicles on the road and also the number of motor vehicle accidents and human fatalities [1].

According to the Highway Statistics 2013 report of the Federal Highway Administration (FHWA), an agency under the United States Department of Transportation (US-DOT). In the period 2012-13, 33,908 people were fatally injured in motor vehicle crashes in the United States [2][3].

Recently a remarkable transformation has happened in ITS and vehicular networks with the emergence of Cloud Computing (CC). This judicious blend of technology is termed as VANET cloud and it promises a new versatile system to enhance transportation efficiency and safety [4][5].

The architectural framework for the VANET cloud is classified into three categories namely Vehicular Cloud (VC), Vehicles using Cloud (VuC), and Hybrid Vehicular Cloud (HVC). Vehicular Ad-Hoc Networks (VANETs) are considered subclasses of Mobile Ad-Hoc Networks (MANETs) [6][8][9].

In vehicular ad-hoc networks (VANETs), vehicles exchange information related to road safety and traffic efficiency via vehicle to vehicle (V2V) or vehicle to infrastructure (V2I) communication. In case the exchanged information is incorrect; accidents and traffic congestion would increase. [10]-[12],[7],[13].

Location closeness is an important variable in VANET, which plays a significant role in the trust model. The location closeness is a procedure to share the position of all neighbouring vehicles with a period of time using all precautions such as; time, safety, and reliability [14].

It also describes the physical position of the actual vehicle with the help of location coordinates using VANET technology. The location closeness is used to verify vehicle information such as vehicle location at a certain time or the area in which the vehicles followed, and use personal information such as user ID and vehicle ID [15].

In location closeness, there are chances of receiving wrong messages or information regarding the vehicles. These attacks are known as "Global Position System Faking Attack"; this attack occurs when the attacker broadcasts fake positioning information which can punish certain applications based on geographical routing, or even nodes located at that same falsified position [8][16].

In addition, "Replayed, Altered, and Injected Messages Attacks" can clearly reduce the performance of all network applications, as well as the exchanged data trustiness.[17].

Therefore, untrustworthy or malicious vehicles increase the chances of transforming insecure information among the vehicles in VANETs. It is a fact that, in VANETs, the overall communication is executed in open access methods, which is the major fact to makes this network vulnerable and post attacks by the attackers. The malicious vehicles can overwrite, modify, and can delete the messages in VANETs. Vehicular Networks System comprises of a number of nodes such as RSU and vehicles. [18][19].Figure.1 shown the rule violated by Pune citizen, Figure .2 show the traffic congestion in camp area in Pune City.

Figure 1: Rule violation by citizens in Pune city

Figure 2: Traffic Congestion in Camp, Pune

2. Literature Survey

In the survey, we studied a proposed method to reduce Vehicle to Infrastructure (V2I) authentication latency and also the distributed public key revocation. For authentication latency, the proposed mobility prediction scheme relies on Multilayer Perceptron (MLP) and an infrastructure-based Short-time Certificate Management (SCM) scheme. This helped to search out out the authentication processing overhead of vehicles at a breaking distance. The proposed novel three-tier vehicular cloud architecture. Tier-1 is named the device level that operates on sensors, repository, knowledge processing, API support, etc. Tier-2 is named the communication level that emphasizes Vehicle to Vehicle (V2V), V2I, and In-car communications. The last level Tier-3 is termed the service level, which works on context, communication, and customized-based services. the facility of the VC concept by enumerating several possible application scenarios. The authors have also discussed several security and privacy issues specific to VCs with possible solutions. This known that Vehicular Cloud Computing (VCC) may be a technologically feasible and economically viable paradigm shift for converging intelligent vehicular networks towards autonomous traffic, vehicle control, and perception systems. the placement closeness is employed to verify vehicles, there are chances of receiving wrong messages or information regarding the vehicles. These attacks are called "Global Position System Faking Attack"; this attack occurs when the attacker broadcasts fake positioning information which might punish certain applications supported geographical routing, or maybe nodes located at that very same falsified position [4], [12]. additionally, "Replayed, Altered, and Injected Messages Attack" is another reasonably attack, which may be defined as "dishonest vehicles can replicate many copies of the identical message, modify the message, or create and inject new messages within the system while acting as a relay node for inter-vehicular communication". These attacks can reduce the performance of all network applications, likewise because the exchanged data trustiness. VANET encounters several security challenges and problems to pander to authentication and privacy securely

[13]. Therefore, untrustworthy or malicious vehicles increase the probabilities of reworking insecure information among the vehicles in VANETs. it's a incontrovertible fact that, in VANETs, the communication is executed in open access methods, which is that the major fact to makes this network vulnerable and post attacks by the attackers. The malicious vehicles can overwrite, modify, and might delete the messages in VANETs.

3. Theory

3.1 Proposed Model

3.1.1 Introduction of Model

As we all know Vehicular ad-hoc networks (VANETs) technology has emerged as a significant research area over the last few years. Being ad-hoc in nature, VANET may well be a mode of networks that are created from the concept of making a network of cars for a specific need or situation. VANET allows vehicles to talk with the roadside equipment.It works under ITS (Intelligent transportation system). Mobile communication, traffic monitoring safety, and

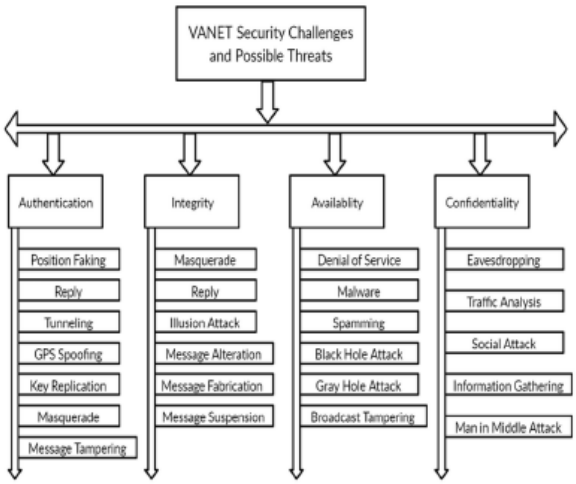

Figure 3: Requirements

public utility management are the key components of VANET. VANETs applications enable vehicles to connect to the online to induce real-time news, traffic, and weather reports but because of a huge increase in population rate the vehicles increase which affects VANET security and privacy so here to scale back the attacks and secure the privacy of VANET we are using 5G integrated VANET trust model which is safer and can help to cut back attacks.

3.1.2 Components of Model

- Requirements:

  It is important in VANET to reduce the security attacks in different infotainment, safety and security-related applications that require the secure exchange of data among nodes. In VANET there are six major requirements as shown below and defined as follows [4], [11],: i. Availability: VANET network should be available to utilize the security, safety, and infotainment application.

ii. Authenticity: This is the most important factor in VANET. It consists of identification, authentication, and access control.

iii. Confidentiality: It enables secure communication between the nodes.
iv. Integrity: It ensures that the node receives the messages in a correct form without alteration or modification.

v. Privacy: The location and identity will keep private and secure.

vi. Non-repudiation: In VANET non-repudiation confirms that the given information sends by a node cannot be denied that it has transmitted.

Figure.3 will show the requirements of this project.

- Drawbacks of VANET Model:

This section listed the common threats faced by VANET [4], [5], [11], also mentioned below:-

I. Certificate Replication Attack: In this attack, the certificate is replicated multiple times. II. Eavesdropping Attack: Attacker intercept transmitted the communication to gain access or password.

III. Tracking Tracing Attack: Trace or track the correct position of device and vehicle.

IV. DoS Attack: it is caused by any action that prevents to access part of a network from functioning correctly and timely manner. This causes a legitimate vehicle to access the application or services.

V. Jamming Attack: This attack is almost the same as a DoS attack, but this time the shared bandwidth among the nodes or network is jammed.

VI. Coalition and Platooning Attack: This attack work in a group where multiple dishonest vehicles collaborate with each other to perform malicious activities such as; bandwidth usage or stopping any services.

VII. Betrayal Attack: This attack occurs when honest vehicles become dishonest during transmission.

VIII. Replayed, Altered, and Injected Messages Attack: This attack altered or modify the information during messages transmission. This will cause to send multiple erroneous messages.

IX. Illusion Attack: Typically this attack is related to hardware component for example wrong sensor reading, incorrect messages are sent to other vehicles.

X. Masquerading Attack: This attack caused by a dishonest vehicle wearing a legitimate certificate by disturbing and doing malicious activities.

XI. Impersonation Attack: A dishonest node assumes to another node by using the wrong identity.

XII. Sybil Attack: A dishonest node transmits multiple fabricated message IDs to the legitimate node where the legitimate nodes assume that they are dealing with multiple devices.

XIII. GPS Position Faking Attack: Falsified positioning based on geographical coordinates.

XIV. Timing Attack: The attacker adds the delay between the packets, which cause unforeseen incidents.

XV. Blackhole Attack: A dishonest node transmits the false reply message to the other vehicle that dishonest host is optimal route information to the destination.

XVI. Gray hole Attack: A dishonest host drops the packet of the particular vehicle in the network and transmits other packets to its destination.

So to overcome these all attacks we are implementing a VANET proposed trust model which overcomes through all these problems.

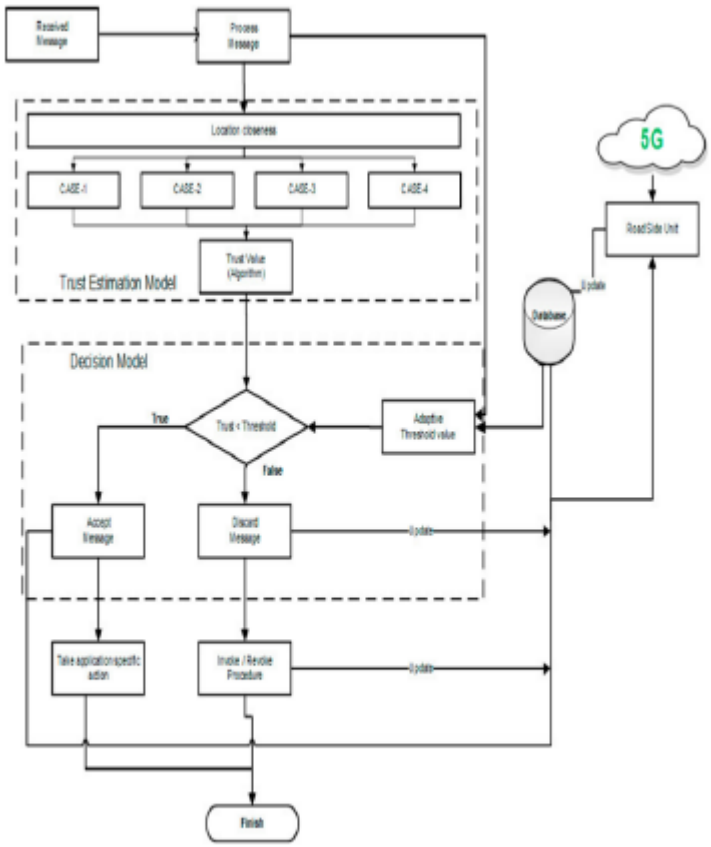

Figure 4: Working of the model

3.1.3 Working of Model

The proposed scenario has been divided into three phases; key exchange, vehicle registration and issue-reporting. The key exchange phase is used by the authorization authorities like CA (Certification Authority), RSU (Road Side Unit) and TPCVC (Traffic Police Controlled Vehicular Cloud) respectively. In

this phase these authorities will generate and exchange a symmetric secret key for their own communication. This key will be different from the key what the authorities will be using to communicate with vehicles on the fly. Vehicle registration phase takes care of the registration of vehicles with CA and TPCVC and as well as the Transient Ticket (TT) generation of vehicle by the RSU. Here the concept of Trust Value (T rV) has been introduced which will be granted by CA to the vehicle for ensuring the trustworthiness of vehicle during communication. Once registered with CA, a maximum of five as (TrV) will be granted to the vehicle. In the issue-reporting phase the sensor values from the vehicle will be reported to the TPCVC and this helps the TPCVC and CA (traffic police department) to initiate action against the vehicle which violated the transport or traffic rule of that region and CA can reduce the (TrV) of the vehicle by one.In figure.4 the working of model is shown.

2) As described above, the proposed trust model consists of two main components; (i)Trust Estimation Model, (ii) Decision Model.

The decision Model in our model received trust value from the trust model to decide whether to process the message or discard it on the bases of the

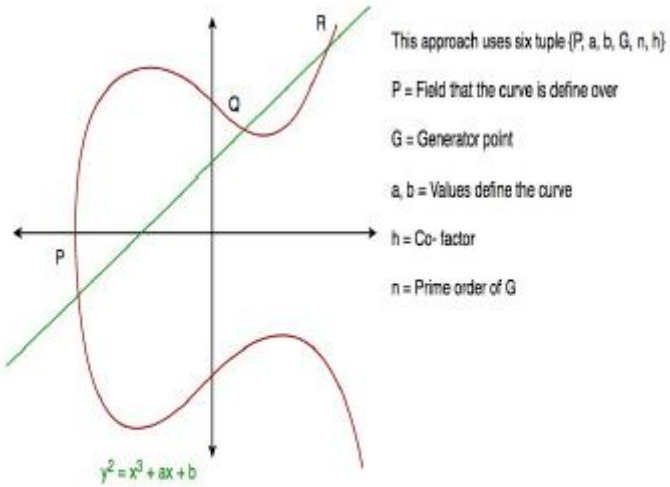

Figure 5: Diffie-Hellman Algorithm Graph

threshold value. If the trust value is less than the threshold value a TRUE message is generated and the decision box accepts the value send an update to a database and takes an application

specific decision. Our Trust Model is for two types of applications that are safety and traffic efficiency.If the trust value exceeds the application-specific threshold value, the message is discarded and the FALSE message is generated.

The false generated message will be discarded and information related to the false message will be stored in the database. Based on the value of the false generated message, invoke/revoke procedure will be executed. Road Side Unit

(RSU) is the trusted unit in the model. RSU will provide initial trust value to all vehicles in the region of interest. All vehicles will have a unique ID in the region. RSU generated an alert message to inform about a malicious vehicle in the region of interest. This alert message helps vehicles in the region not to trust the information received from the malicious node.1.

3.2 Algorithm

3.2.1 Diffie–Hellman (DH) Algorithm

It is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the Internet. DH enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric cryptography.Figure.5 explain the graph of Dillie-Hellman Algorithm.

Algorithm

Step1: Alice and Bob get public numbers P=23, G=9

Step2: Alice selected a private key a=4 and bob selected a private key b = 3

Step3: Alice and Bob compute public values

Alice: x= $(9^4 mod 23) = (6561 mod 23) = 6$

$Bob : y = (9^3 mod 23) = (729 mod 23) = 16$

$Step4 : AliceandBobexchangespublicnumbers$

$Step5 : Alicereceivespublickeyy = 16and$

Figure 6: Working of RSA

$Bobreceivespublickeyx = 6$

$Step6 : Aliceandbobcomputesymmetrickeys$

$Alice : ka = y^a modp = 65536 mod 23 = 9$

$Bob : kb = x^b modp = 216 mod 23 = 9$

$Step7 : 9isthesharedsecret.$

3.2.2 RSA

It is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public key and Private key. As the name describes that the public key is given to everyone and private key is kept private. Figure.6 explain you the WOrking of RSA.

Algorithm

1) Generating Public Key

• Select two prime no's. suppose p = 53 and Q = 59.

Now first part of the public key : n = P*Q = 3127.

• We also need a small exponent say e:

But e must be

- An integer.
- Not be a factor of n.
- 1¡e¡ (n)

Let us now consider it to be equal to 3

• Our Public Key is made of n and e.

2) Generating Private Key

• We need to calculate (n):

such that (n) = (P-1)(Q-1)

so, (n) = 3016

• Now calculate Private Key, d:

d=(k*(n) +1) / e for some integer k

For k=2, value of d is 2011

4. Advantages

The promise of safe driving, intelligent traffic system, early warning signals for motorists that would minimize road mishaps, increase road conditions advisement, and provision of higher in-transit communication, inter-vehicle communication, and road-vehicle communication are a number of the hallmark of auto spontanepous network (VANET). VANETs are wont to provide communications to nearby vehicles in terms of V2V and vehicles. This VANET application is referred as a non-safety application, which aims at enhancing drivers and passenger's comforts. It can provide the motive force and passenger with the updated climate information, hotels, nearby restaurant, and patrol stations. Passengers can play games online, get Internet access, and send and receive messages when vehicle is within the range of the network. The safety applications of VANETs are accustomed enhance the protection. In this safety application, vehicle-to-vehicle and/or vehicle-to-infrastructure communications will be accustomed improve the traffic safety, lane changing warning, emergency video streaming, avoiding collisions, and accidents. The main purpose of this application is to make sure the protection of drivers, passengers, and pedestrians.

5. Conclusion and Future work

Secured Vehicular Ad-hoc Network (VANET) cloud communication in Intelligent Transport Systems (ITS) may be a challenging task. during this paper, a secured VANET cloud-based application for detecting transport or traffic rule

violations when the vehicle is on the move is proposed. This helps the traffic local department to enhance road traffic productivity with the utmost safety. The concept of car Using Cloud (VuC) is employed during this work to store messages, keys, certificates, and sensor values. The proposed Trust Value (TrV) and RSU generated Transient Ticket (T T) have contributed to the improved reliability of this application by providing unconditional trust in vehicles and reducing communication latency. additionally to the present, the importance of VANET security and also the list of common threats which will be attacked on VANET are described. Moreover, the concept of integrating 5G within the proposed model means establishing the method with higher bandwidth to secure the vehicular ad-hoc network. Therefore, this research proposed a model for measuring quot;location closenessquot; through two main blocks (Trust Model and Decision Model) for executing and transmitting messages between the nodes. This paper is beneficial for establishing a secured community with the assistance of the proposed trust model. This was specifically supported calculating the quot;Location Closenessquot; parameter.

Further research will focus on how to seamlessly adapt security schemes in the vehicular cloud with a prioritised message dissemination service in VANET cloud communication. The communication overhead and security performance will be investigated by simulating more realistic scenarios, and the proposed model will be enhanced by adding other parameters such as data integrity and authentication.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8] B. Mokhtar, "Survey on security issues in vehicular ad hoc networks," Alexandria Eng. J., vol. 54, no. 4, pp. 1115–1126, 2015. .

[9] Q. Alriyami, A. Adnane, and A. K. Smith, "Evaluation criterias for trust management in vehicular ad-hoc networks (VANETs)," in Connected Vehicles and Expo (ICCVE), 2014 International Conference on, 2014, pp. 118–123..

[10] B. Donnellan, C. Klein, M. Helfert, and O. Gusikhin, Smart Cities, Green Technologies and Intelligent Transport Systems: 7th International Conference, SMARTGREENS, and 4th International Conference, VEHITS 2018, Funchal-Madeira, Portugal, March 16- 18, 2018, Revised Selected Papers, vol. 992. Springer, 2019. .

[11] M. S. Al-Kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," in Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on, 2012, pp. 1–9. .

[12] Ashritha, M., Sridhar, C.S., 2015. RSU based efficient vehicle authentication mechanism for VANETs. IEEE 9th International Conference on Intelligent Systems and Control (ISCO), pp. 1–5.

[13] Jarp, S., Bechler, M., Wolf, L., 2005. Evaluation of routing protocols for vehicular Ad Hoc networks in typical road traffic scenarios. Proceedings of the 11th EUNICE Open European Summer School on Networked Applications, pp. 584–602..

[14] U. Ihsan, S. Yan, and R. Malaney, "Location Verification for Emerging Wireless Vehicular Networks," IEEE Internet Things J., 2019. .

[15] J. Zhang, "A survey on trust management for vanets," in Advanced information networking and applications (AINA), 2011 IEEE international conference on, 2011, pp. 105–112..

[16] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust modeling framework for message propagation and evaluation in VANETs," in Information Technology Convergence and Services (ITCS), 2010 2nd International C.

[17] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," Veh. Commun., p. 100179, 2019..

[18] D. M. West, "How 5G technology enables the health internet of things," Brookings Cent. Technol. Innov., vol. 3, pp. 1–20, 2016..

[19] R. Canetti, J.D. Tygar, D. Song, The TESLA broadcast authentication protocol, RSA CryptoBytes, vol. 5.