IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 9, September 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 9, September 2024| DOI: 10.15680/IJIRCCE.2024.1209011

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Data-Centric Misbehaviour Detection and Safety Applications in Vehicular Ad Hoc Networks and Optimal RSU Replacement

Dr.Nalina V[1], Dr.P.Jayarekha[2]

Assistant Professor, Department of ISE, BMS College of Engineering, Bangalore, India[1]

Professor and Head, Department of ISE, BMS College of Engineering, Bangalore, India[2]

ABSTRACT: The paper focuses on the challenges and solutions in the context of vehicular ad hoc networks (VANETs), particularly in terms of misbehaviour detection and optimal RSU replacement. It outlines the need for accurate information sharing among vehicles for safety and assistance purposes. The paper introduces a data-centric approach for detecting misbehaviour in VANETs, emphasizing the detection of incorrect information rather than classifying nodes as "good" or "bad." The proposed approach utilizes pseudonyms for location privacy and aims to be resilient against Sybil attacks. The concept of the proposed method is to issue fines based on the number of erroneous messages sent, rather than revoking nodes entirely. It discusses the various applications of VANETs, particularly safety applications such as post-crash notifications and road hazard alerts. Experimental results and analysis demonstrate the performance of the proposed approach.

KEYWORDS: VANET; RSU, Urban Mobility; Multi-criteria optimizations; Convolutional neural network CNN.

I. INTRODUCTION

Driving involves constantly changing locations. There is a constant demand for information about the current location and more specifically about nearby traffic, routes, etc. There are certain categories in which these details can be categorized. The safety and assistance of drivers is a very important category. It includes a variety of things that are mostly determined by data sensed from other cars. It is possible to think of brake warnings from cars ahead, collision warnings, tailgate warnings, information about road maintenance and conditions, traffic jam warnings, detailed regional weather forecasts, warnings about accidents behind the next road, detailed information to rescue teams about accidents and many other details. People feel the need to keep up with local traffic scenarios and follow any driver. It helps to update things in the system. Another category is infotainment for passengers. Chatting between military cars in war scenarios, updating the nearby vehicles, and parking in a free space in shopping malls using a parking system.

The youngsters will enjoy it. Drivers on the roadway are alerted to oncoming petrol bulk and parking zones. There is a vehicle healing system in cars that indicates incorrect spares and alerts the driver to double conditions. As a result, the driving force will react to the problem inside the vehicle.

However, study is being undertaken. Ad hoc vehicular transportation NETworks (VANETs) are a sort of cellular ad hoc community (MANET) that attempts to enable communications between adjacent automobiles (also known as inter-car communication -(IVC)-) and between automobiles and neighboring roadside base-stations (also known as car-to-roadside conversation -(VRC)-).

The application area for vehicle-to-automobile and car-to-roadside verbal contact is large, providing for excellent economic potential and the analysis of complex situations. VANETs are expected to help with the
(1) protection-associated programs
(2) Comfort applications.

Despite the fact that the academy and industry have concentrated research efforts on security-related applications because of their significance for the automobile domain, it's far anticipated that research on consolation programs (as it

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

offers high-quality commercial enterprise opportunities) will continue to entice designers and researchers to broaden non-security VANET-based totally packages. The VANET system might be supported by the modern payment technique built using the IP-based community to allow bills in automobiles. The scenario described above can be represented in the actual world by using the following example: a customer is driving and stops at a gas station to buy fuel or a few other things within the fuel station can be stored with a small amount of fee card. If the client node is unable to communicate with the cardboard company from the software unit (due to a lack of essential components such as a HotSpot (HS)-), the road-facet gadgets (RSUs), or the purchaser must nonetheless be able to carry out the fee utilizing the service provider's infrastructure. The connectivity scenario depicted in Fig. 1 is an illustration of the aforementioned circumstance, in which a car (henceforth referred to as the customer) is equipped with an On-stand Unit.

An OBU and an application Unit (AU) can only interact with the service provider during a charge transaction due to a lack of internet access with its AU. However, because this research is outside the scope of this paper, we will provide any test that demonstrates that the proposed protocol works properly while the client is in the flow. Many strategies were investigated to enable authentication in digital fee systems (including cellular trading), but symmetric and uneven signature approaches were adopted. Traditional uneven signature methods, on the other hand, make signature computations exceedingly expensive and are not ideal for transportable gadgets (including those typically attached to an OBU) now on the market that are not based on the Texas contraptions TMS620C55x processors family. The protocol we suggest for these artworks is intended for situations in which there is no direct communication between the consumer and the cardboard company. As a result, because the customer has connectivity limits, communication with various events (such as this sort of Certification Authority, for checking a certificate) isn't possible throughout a payment process. As a result, to meet the requirements of the protocol presented in this work, the assistance of a symmetric signature method is required. Symmetric cryptography (the use of a shared key between two events) permits message secrecy, message integrity, and birthday party authentication, and is a viable choice for developing secure protocols for cellular pricing systems. Symmetric-key operations no longer require massive amounts of processing resources or extra communication steps (as in protocols based completely on public-key infrastructures, where a public-key certificate must be validated by a certificate Authority). To prevent the error of direct contact between the card issuer and the customer for authentication functions, we devised and implemented a charge protocol that allows the consumer to send a message to the card company via a service provider (the merchant will not be able to decrypt the message). The Kiosk Centric Version Protocol for VANETs (henceforth referred to as the KCMS-VAN Protocol) proposed protocol uses symmetric-key operations in all interested parties to reduce both transaction setup and infrastructure costs. Furthermore, it simplifies debit and credit card transactions, protects the customer's identity at some point during the transaction, and must be used in conjunction with a portable tool linked to an AU. Using real cellular phones and PDAs as implementation platforms, we assess the performance of the KCMS-VAN protocol. This allows us to show that our consumer-side application can be installed on a variety of Java TM-enabled memory-constrained transportable wireless handheld devices.

Every day, our motors make use of advanced computational technologies, mostly for safety reasons. The UCLA Vehicular community Lab was established as one of the pioneers in displaying autos as wireless community nodes travelling through traffic automobile-to-automobile communication converts automobiles from mere transportation means to smart things. Vehicle-to-vehicle communication, according to [EiSc06], permits several new motor goods and opens up numerous choices for security enhancements. It can be used to incorporate active safety and driver support services such as real-time traffic, collision warning, and active navigation structures, as well as climatic information. Researchers are encouraged to investigate the behaviours of automobile networks and cars as a result of these blessings. Automobile-to-car communication networks are sometimes known as vehicular networks. There are two types of vehicle networks that could be prominent. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. V2I refers to communication between motors and a fast verbal interchange infrastructure, whereas V2V refers to communication among vehicles. VANET represents (1) the verbal exchange between vehicles (V2V) and (2) the verbal exchange between cars and roadside devices (RSUs) when they use the same ad hoc wi-fi technology, which includes IEEE 802.11p [IEEE802.11p-2010]. An RSU is a fixed base station.

This is located on the side of a road. OBU (On Board Unit) is an automobile module that aids in the verbal communication of a vehicle with roadside gadgets, other motors, and infrastructure. In this case, a car accident has

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

happened at an intersection, and VANET is being utilized as a V2V communication network to warn cars in the neighborhood about the event.

VANET transforms each participating vehicle into a wireless router or node, allowing motors 100 to 600 meters distant to join and establish a network with a wide range.

II. LITERATURE SURVEY

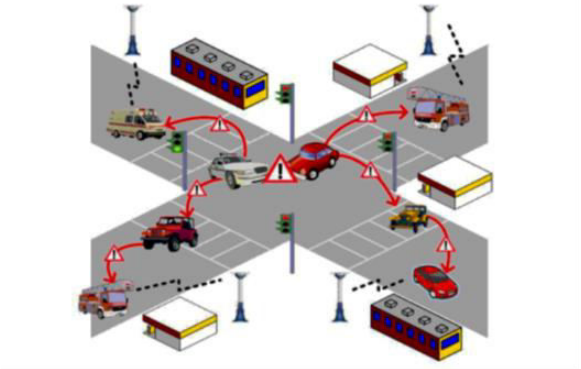
This study explores the realm of Vehicular Ad Hoc Networks (VANETs) and their potential to enhance road safety and comfort. Given the profound influence of VANET-transmitted data on vehicle behavior, the demand for robust security is evident. Building upon existing research, this paper offers a comprehensive examination of misbehavior detection in VANETs. It begins by dissecting VANET characteristics, security challenges, and prevalent attack vectors. The subsequent sections precisely define misbehaviour, its detection modes, and the entities involved. The study categorizes generic misbehaviour detection into data-centric and node-centric approaches. In a VANET-specific context, a novel taxonomy for misbehaviour detection is proposed, emphasizing the interplay between vehicles, detection modes, and participants. Lastly, the paper addresses remaining concerns, open issues, and charts potential future research directions in this crucial domain.[11]

This paper explores the significance of Vehicular Ad-Hoc Networks (VANETs) in the context of Intelligent Transportation Systems (ITS) as a means to enhance road safety and alleviate traffic congestion. VANETs rely on cryptographic techniques to ensure message integrity and vehicle authentication, yet they remain vulnerable to insider attacks. Specifically, the injection of false position data into basic safety messages (BSMs) by misbehaving vehicles can have severe consequences, including accidents and traffic disruptions.

To address this challenge, the paper introduces a novel data-centric approach that leverages machine learning (ML) algorithms for the detection of position falsification attacks. Unlike existing methods, this approach utilizes information from two consecutive BSMs for both training and testing. Through simulations conducted with the Vehicular Reference Misbehavior (VeReMi) dataset, the proposed model demonstrates superior performance in identifying various attack types, highlighting its potential to enhance VANET security significantly.[12]

III. ALGORITHM

The transition chance matrix is dynamic and subject to change. The "mobility model" is the instantaneous fee of the transition probability matrix at any point in time.



1. The loose glide mobility version P, which depicts the motive force's behaviour in the absence of a crash.
2. T is the crash-website mobility variant that applies when the car simply passes by the stated crash-website.
3. A weight (t) showing the proximity of the driver's mobility version to the crash-website online mobility version. The mobility model at each intermediate time factor is considered to be a linear combination of P and T, and the parameter is presented in such a way that the mobility model that applies at time t is (1 - (t))P + (t)T if a crash has happened.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. M(t) = (1-α(t))If a crash has occurred, P +(t)T is the mobility version that applies at time t. As a result, if the driver understands whether the PCN alert is valid or incorrect at the time of reception, the mobility version is defined as M(t) if the alert is correct and P if the warning is false.
(xt', yt') and (xt, yt), the distance d is calculated as d = where t0 is the time when the car arrives at the crash scene. Misbehavior is declared if d exceeds the stated threshold of $.

IV. PROPOSED SYSTEM

In this section, we focus on approaches that aim to improve VANET safety using architectural and systematic methodologies. This debate also includes unusual assaults and cryptography solutions.

User privacy is protected by an identification-based security device.
Authentication, integrity, and non-repudiation should be fundamental VANET security criteria. In a few exceptional circumstances, confidentiality must be provided in resistance to attackers. Furthermore, person privacy, as well as identification and location records, are sensitive facts that must be protected against illegal tracking and consumer profiling for marketing. In other cases, clients may not accept VANET technology due to financial considerations. Similarly, law enforcement authorities continue to exploit legal responsibility problems in relation to crimes or injuries and seek some degree of traceability of autos. Almost all of the VANET administration is devoted to retaking the role of misbehaving users. Even though it is relatively simple to deny access to unauthorized misbehaviours because their communication requests can be rejected by nearby customers and roadside gadgets, the misbehaviour CMS-van of official customers is more complex and difficult because those legal customers have credentials and may pass through authentication procedures.

The gadget's concept, in particular, warrants the privacy machine, which holds the authentication threshold. Furthermore, the threshold will indicate misconduct and result in the user's credentials being revoked. Similarly, the device employs a dynamic accumulator for the privacy approach, which places further constraints in threshold on other speaking clients. These are especially appealing to service providers since they could benefit from increased efficiency in their products. Figure suggestions on specific security challenges: This section describes suggestions that primarily focus on a specific area of VANET security, such as role detection, modeling attacks, integrity assessment, and anti-jamming measures.

VANETs are popular because they can considerably improve road safety and the use of rules. Detecting misbehaviour in VANETs may be critical because it is risky. This survey's purpose is to provide an overview of the various malpractice detection methods utilized in VANETs..

This survey is intended to be useful for researchers interested in VANET malpractice detection techniques, as well as to mitigate other studies to make VANET more secure. Misbehaviour detection strategies have been classified as Node-Centric and Fact-Centric. Furthermore, such solutions have unique difficulties that must be addressed in order to improve the dependability and relaxation of VANET. In a data-centric technique, detection performed through the use of security alert messages lowers the additional overhead concerned in the use of sensors and extra message communication. However, if the cost of the received statistics is not always assessed quickly, the message may become ineffective [6]. As a result, effective processing devices must be installed in automobiles. In order to detect misbehaviour, efficient learning algorithms can be used to extract the correct linkage of events and courting among vehicular nodes. It has been discovered that no single MDS is capable of detecting all types of misbehaviour in VANETs. As a result, future hybridization of facts-centric and node-centric systems to integrate the benefits of both techniques may be witnessed. This method will aid in the detection of more complex attacks. Drivers and motors in VANET must provide their id to RSUs in order to communicate with them. However, the privacy and security of such documents must be handled with extreme caution to avoid misuse by attackers [4].

V. EXPERIMENT RESULT & ANALYSIS

VANETs can be used for a wide range of non-safety and safety applications, including automated toll payment, vehicle safety, traffic management, enhanced navigation, location-based services like locating the nearest fuel station, travelodge, or restaurant, and infotainment applications like Internet access[4].

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

There are three main types of VANET applications.

- Commercial application: In this application, the VANET is utilized to provide commercial services such as streaming audio and video, internet access, and so on.
- Convenience application: In this application, OBUs interact with other vehicles and infrastructure points to give the driver with services such as traffic flow information, parking availability information, automatic toll payment, and so on.
- Safety application: The VANET is utilized in this application to discover circumstances that could risk the drivers' safety.

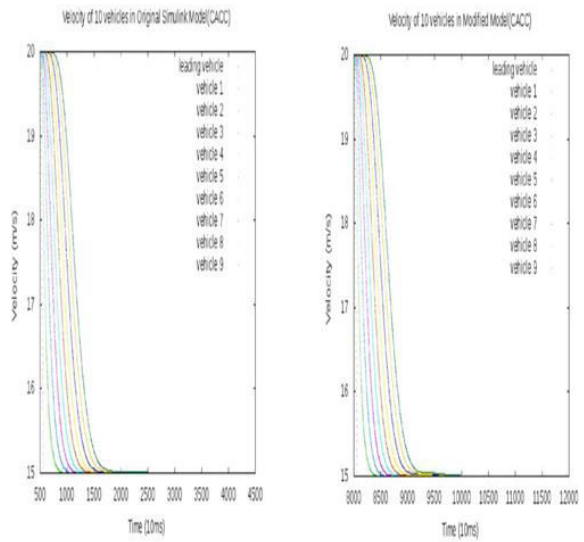
This thesis will be entirely focused on safety applications. The following are some examples of VANET safety applications:

1.**Post-Crash Notification**: When a vehicle is involved in a collision, it sends a PCN warning to the automobiles in its vicinity, informing them of the crash's existence and location and allowing them to take evasive action.

2.**Slow or Stopped Vehicle Advisory**:An SVA alarm is sent by a vehicle that abruptly slows or stops on the road, allowing listeners to take evasive action once more.

3.**Road Hazard situation Notification**: When a vehicle sees a potentially hazardous situation on the road, such as road slipperiness, it broadcasts a RHCN alert to notify other motorists.

4.**Road Feature Notification**: When a vehicle detects a road feature, such as a sharp curve or a slope, that necessitates corrective action by the driver, it communicates an RFN alert to neighbouring vehicles [8].



(a) The velocity of ten cars in the Original Ns3 Simulator Model (CACC). (b) Modified Model (CACC) velocity of ten cars

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

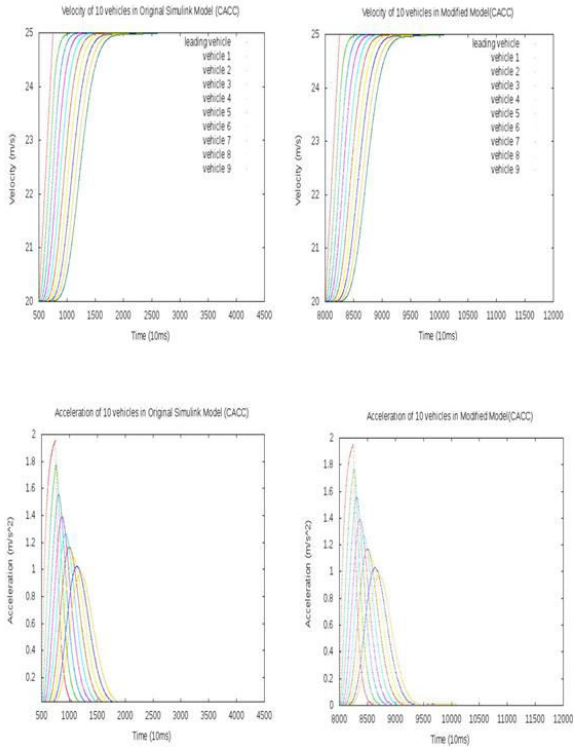


Figure: velocity and acceleration of 10 vehicles in Original Ns3 Simulator Model and modified (accelerating scenario

VI. CONCLUSION

We reviewed the shortcomings of existing VANET misbehavior detection techniques and presented a new one. We introduce the concept of data-centric MDS, in which we are more interested in discovering incorrect information than in categorizing nodes as "good" or "bad." The major rationale for this is that nodes misbehave for selfish reasons and do not need to be classified as "good" or "bad" nodes. By using pseudonyms, we may provide location privacy. By watching the location of the node after issuing an alert, any node can detect erroneous alert information [6]. Voting and majority decisions are unnecessary. As a result, our approach is resistant to Sybil attacks. As a result, we do not entirely revoke nodes, but instead issue fees based on the number of erroneous messages sent out. We highlight some of our scheme's drawbacks and offer several future research prospects [8].

REFERENCES

1. J. L. Abad Peiro, N. Asokan, M. Steiner, and M. Waidner (1997). Creating a general payment service. 72-88 in IBM Systems Journal, 37(1).
2. Asokan (1994). In a mobile computing environment, anonymity is important. In Mobile Computing Systems and Applications Workshop (pp. 200-2004).
3. Bella, G., and S. Bistarelli (2005). Security protocols require information assurance. Computers and Security, vol. 24(4), pp. 322-333.
4. Bellare (2006). New NMAC and HMAC proofs: security without collision resistance. Crypto 2006, the 26th annual international cryptology conference (pg. 602-619).
5. M. Bellare, J. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, Els. Van Herreweghen, and M. Waidner. The iKP secure electronic payment system was designed, implemented, and deployed. 18(4), 611-627, IEEE Journal on Selected Areas in Communication.
6. Certicom (2003a). Cryptography's next generation. Certicom's Bulletin of Security and Cryptography, 1 (1), Code and Cipher.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

7. Car2Car Communication Consortium. C2C-CC system overview (Technical Report version 1.0). Consortium for Car-to-Car Communication.
8. S. Chari, P. Kermani, S. Smith, and L. Tassiulas (2001). A usage-based taxonomy of security problems in M-commerce. Agents of e-commerce (pg. 264-282).
9. Hassinen, K. Hyppönen, and K. Haatajam (2006). A mobile payment system that is open and PKI-based.International conference on Emerging Trends in Information and Communication Security (ETRICS' 2006), pp. 86-100.
10. Hu, Z., Liu, Y., Hu, X., and Li, J. In a mobile data network, anonymous micropayments authentication (AMA) is used. IEEE INFOCOM, 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (pp. 46-53).
11. Xiaoya Xu, Yunpeng Wang, Pengcheng Wang, "Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks", Journal of Advanced Transportation, vol. 2022, Article ID 4725805, 2022.
12. A. Sharma and A. Jaekel, "Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach," in IEEE Open Journal of Vehicular Technology, vol. 3, pp. 1-14, 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details