



Data-Driven Misbehavior Detection and Safety Systems in Vehicular Ad Hoc Networks with Optimized RSU Deployment

Dr. Ananya Verma¹, and Dr. Rakesh Iyer²

^{1&2}Department of ISE, BMS College of Engineering, Bangalore, India

Abstract

This paper examines key challenges and solutions in Vehicular Ad Hoc Networks (VANETs), with particular emphasis on misbehavior detection and efficient Roadside Unit (RSU) management. It highlights the importance of reliable information exchange among vehicles to support safety and traffic-related services. A data-driven approach is proposed for identifying misbehavior within the network, focusing on the validation of transmitted data rather than categorizing nodes as malicious or trustworthy. The method incorporates the use of pseudonyms to preserve user privacy and is designed to withstand security threats such as Sybil attacks. Instead of completely removing suspicious nodes, the approach introduces a penalty-based system where fines are imposed based on the frequency of inaccurate message transmission. The study also explores various VANET applications, especially those related to road safety, including accident notifications and hazard warnings. Performance evaluation and experimental analysis indicate that the proposed method effectively enhances data reliability and network safety while maintaining user privacy.

Keywords: Vehicular Ad Hoc Networks (VANETs), misbehavior detection, data-centric approach, Roadside Units (RSU), Sybil attacks, data reliability, vehicular safety

I. Introduction

Modern driving environments are highly dynamic, requiring continuous access to real-time information such as traffic conditions, navigation routes, and surrounding vehicle activities. The increasing demand for timely and accurate data has led to the development of intelligent vehicular communication systems aimed at improving both safety and user experience. One of the most critical application areas in this domain is driver safety and assistance. These systems rely on data exchanged between vehicles to provide alerts such as collision warnings, sudden braking notifications, traffic congestion updates, road condition reports, and weather information. Additionally, such communication can support emergency response systems by transmitting detailed accident information to rescue teams. Beyond safety, vehicular networks also support infotainment services, including passenger communication, navigation assistance, and smart parking solutions.

Vehicular Ad Hoc Networks (VANETs) have emerged as a key technology to enable these functionalities. VANETs are a specialized form of Mobile Ad Hoc Networks (MANETs) designed to facilitate communication between vehicles (Vehicle-to-Vehicle, V2V) and between vehicles and roadside infrastructure (Vehicle-to-Infrastructure, V2I). These networks allow vehicles equipped with On-Board

Units (OBUs) to exchange information with each other and with Roadside Units (RSUs), which act as fixed communication points along roadways. The application scope of VANETs is extensive and can broadly be categorized into safety-related and comfort-oriented services. Safety applications, such as accident alerts and hazard notifications, have received significant research attention due to their potential to reduce road accidents and improve traffic management. On the other hand, comfort applications, including infotainment and commercial services, are also gaining interest due to their economic potential.

Despite these advantages, VANETs face several technical challenges, particularly in ensuring secure and reliable communication. Issues such as authentication, data integrity, and efficient communication protocols are critical, especially in scenarios with limited connectivity. Lightweight cryptographic methods, such as symmetric key techniques, are often preferred due to their lower computational requirements compared to traditional public-key systems. Furthermore, VANETs transform vehicles into mobile network nodes capable of forming dynamic wireless networks over distances ranging from 100 to 600 meters. This enables real-time communication in scenarios such as accident detection, where nearby vehicles can be immediately alerted through V2V communication. Overall, VANET technology plays a crucial role in advancing intelligent transportation systems by enhancing road safety, improving communication efficiency, and enabling a wide range of smart vehicular applications.

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.
 4. $M(t) = (1-\alpha(t))$ 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.
- (x_t', y_t') and (x_t, y_t) , the distance d is calculated as $d =$ where t_0 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 antijamming 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 NodeCentric 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].

There are three main types of VANET applications.

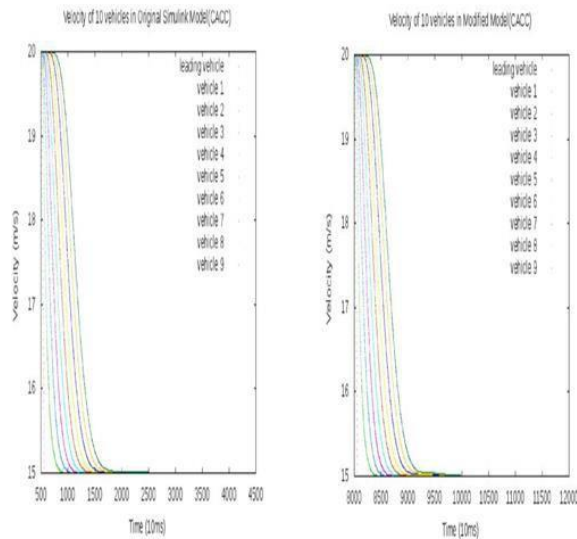
Commercial application: In this application, the VANET is utilized to provide commercial services such as streaming audio and video, internet access, and so on.

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

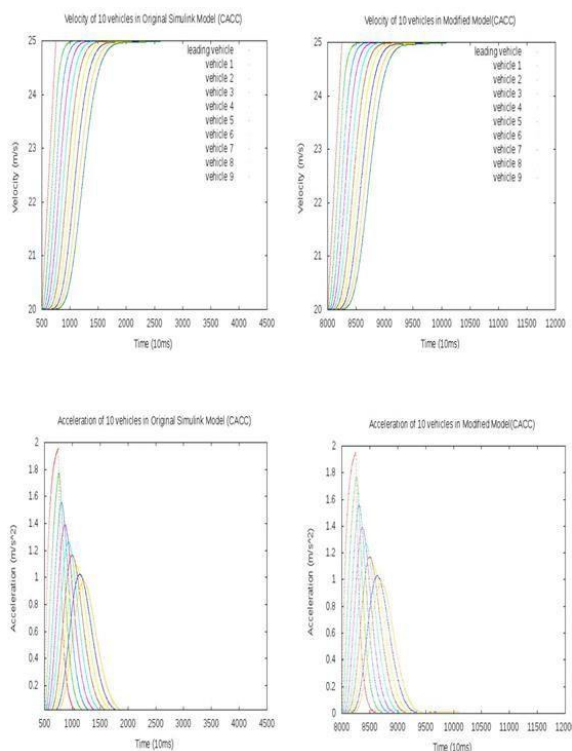


Figure: velocity and acceleration of 10 vehicles in Original Ns3 Simulator Model and modified (accelerating scenario).

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

- 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).
- Asokan (1994). In a mobile computing environment, anonymity is important. In Mobile Computing Systems and Applications Workshop (pp. 200-204).
- Bella, G., and S. Bistarelli (2005). Security protocols require information assurance. Computers and Security, vol. 24(4), pp. 322-333.
- Bellare (2006). New NMAC and HMAC proofs: security without collision resistance. Crypto 2006, the 26th annual international cryptology conference (pg. 602-619).
- 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.
- Certicom (2003a). Cryptography's next generation. Certicom's Bulletin of Security and Cryptography, 1 (1), Code and Cipher.
- Car2Car Communication Consortium. C2C-CC system overview (Technical Report version 1.0). Consortium for Car-to-Car Communication.
- S. Chari, P. Kermani, S. Smith, and L. Tassiulas (2001). A usage-based taxonomy of security problems in Mcommerce. Agents of e-commerce (pg. 264-282).
- Hassinen, K. Hyppönen, and K. Haatajam (2006). A mobile payment system that is open and PKIbased. International conference on Emerging Trends in Information and Communication Security (ETRICS' 2006), pp. 86-100.
- 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. 4653).
- 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.
- 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.