Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 45 No. 4
April 2024

A Robust Solution for Jammer Localization and Avoidance in Vehicular Ad-Hoc Networks

[1]Dr.N.M Saravanakumar , [2]Atchaya R., [3]Bala Murali Krishnan V., [4]Gothai V., [5]Vidhyalakshmi A.,
[1]M.E.,Ph.D
Department of IT Karpagam College of Engineering Coimbatore,India
[2]Department of IT Karpagam College of Engineering Coimbatore,India
[3]Department of IT Karpagam College of Engineering Coimbatore,India
[4]Department of IT Karpagam College of Engineering Coimbatore,India
[5]Department of IT Karpagam College of Engineering Coimbatore,India

Abstract— The phrase vehicular ad hoc networks(VANET) refers to vehicle nodes that provide various services such as accident avoidance, traffic management. In vehicles, it is essential to send/receive messages without any interruptions. The innovative developments in vehicles have converted traditional vehicles into intelligent devices that provide convenience and safety. Vehicular Ad Hoc Networks (VANETs) hold great promise for enhancing road safety and traffic management by enabling vehicles to communicate with each other and with roadside infrastructure. This project presents an innovative approach to address the problem of jamming attacks in VANETs through efficient localization and avoidance. The system continuously monitors the wireless communication environment within the VANET. Our method leverages the inherent mobility of vehicles in VANETs to dynamically detect and localize jamming sources. Once a jamming source is localized, our system implements intelligent avoidance strategies. It dynamically reroutes affected vehicles around the jammed area by utilizing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications.
Keywords— *Ad-Hoc Networks, VANETS, Adaptive routing.*

Introduction

Networking, in the context of information technology, refers to the practice of creating connections between computers, devices, or systems to facilitate communication and resource sharing. It involves the design, implementation, and management of the infrastructure that enables data exchange and collaboration.

The term Vehicular Ad Hoc Networks (VANETs) has ushered in a new era of connectivity and data exchange among vehicles and roadside infrastructure, promising to revolutionize road safety, traffic management, and transportation efficiency. Transportation is reshaped by the advancement of vehicles. VANETs facilitate the exchange of traffic information among vehicles and infrastructure, enabling drivers to receive real-time updates about accidents,

road closures, and alternative routes. The proposed method aims to efficiently detect and localize jamming sources in VANETs, leveraging the dynamic nature of vehicular mobility.

Security remains a primary concern, with the susceptibility to jamming attacks posing a significant threat. The attacker's mission is more accessible due to the network's open nature, way of communication, and lack of security measures. Constant changes in vehicle positions and rapid network topology alterations contribute to packet loss and delays, affecting communication quality. Vanet's are specifically designed to enable vehicles to communicate seamlessly with each other and with roadside infrastructure, creating an ad-hoc and dynamic network on the go. Equipped with Roadside Units (RSUs), these networks facilitate real-time information exchange, enhancing road safety, traffic management, and overall driving experience. In an era marked by rapid technological advancements and the ever-increasing demand for efficient and secure transportation systems.

Proposed approach uses Ciphertext Policy Attribute-Based Encryption (CP-ABE) is an advanced encryption scheme that combines attribute-based encryption and ciphertext access policies. ABE is a type of public-key encryption where access to encrypted data is based on attributes, such as user

characteristics or properties. VANETs are a subset of Mobile Ad Hoc Networks (MANETs) that enable vehicles to communicate with each other and with roadside infrastructure without the need for a pre-established infrastructure or central authority.

Existing approach uses the signal strength of the jammer for estimating only the distance between jammer and receiver and a less complex algorithm is proposed for localizing the jammer and then redirecting the vehicles away from the road. So the proposed approach provides the security to the data owner and the receiver who can access the data based on certain attributes. CP-ABE provides a level of privacy for both data owners and users. In a traditional ABE scheme, encryption policies are tied to the attributes, and only users with matching attributes can decrypt the data. The innovative developments in autonomous vehicles have converted traditional vehicles into intelligent devices that provide convenience and safety.

However, this heightened interconnectivity necessitates robust security and privacy measures to protect the sensitive information transmitted within these networks.

I. Motivation Contribution

The main issues identified are listed below,

1. Estimate the relative speed of a mobile vehicle that inter- feres with RF communication of a transmitter-receiver pair and the proposed method is Radio frequency (RF), angle of projection (AOP).
2. Develop an Intrusion Detection System to detect spoofing attacks by utilizing Machine Learning techniques to protect electric vehicles and the proposed method is K-NN, RaFo.
3. Classify the jamming at- tack type by employing Delivery Ratio (PDR) and Received Signal Strength (RSS) to train several machine learning algorithms and the proposed method is Gradient Boosting, KNN, RaFo, DT.
4. Deploy supervised learning (KNN, RaFo) in developing a detection scheme by utilizing the variations of relative speed and the proposed method is K-NN, RaFo.
5. Utilize unmanned aerial vehicles (UAVs) in observing the communication status by implementing Q-learning analysis and the proposed method is Q-learning analysis.
6. Propose a hide away anti- jamming strategy for VANET infrastructure and the proposed method is Channel Surfing and Hideaway.
7. Locate the jammed nodes in broadcast networks by collecting the MAC-layer statuses of the jammed nodes at the physical layer and the proposed method is the number of jammed slots (NJS).
8. Utilize the jamming strength in a geometric-covering method in order to localize the jammer and the proposed method is GJL.
9. Constant changes in vehicle positions and rapid network topology alterations contribute to packet loss and delays, affecting communication quality and the proposed method is RSU to Central controller communication distance.
10. Privacy measures to protect the sensitive information transmitted within the networks and the proposed method is CP-ABE.

Based on the proposed methodology, it has been determined that the primary factor contributing to all identified issues is the separation distance between the Roadside Unit (RSU) and the vehicle, influencing the efficacy of communication between the sender and receiver. Identifying the issues mentioned above has played a key role in attaining improved communication accuracy. Consequently, this enhancement in accuracy results in increased overall efficiency when compared to existing methods and approaches.

II. Existing System

Jamming is a formidable assault that poses a threat to vehicular communications based on the 802.11p standard. This attack involves inundating the network with jamming packets, thereby occupying the communication channels. The consequences of such an attack are particularly alarming for self-driving cars, as uninterrupted message transmission is crucial for remote vehicle control. In the context of wireless vehicular ad hoc networks (VANET), the attacker finds it easier to carry out their mission due to the open nature of the network, the mode of communication, and the absence of security measures. While existing studies have primarily focused on detecting jamming attempts, few have addressed the challenge of localizing the jammer. Furthermore, even in these limited studies, the assumptions underlying the proposed countermeasures and

their complexity have been overlooked. Consequently, this paper presents a novel approach that efficiently detects, localizes, and mitigates jamming attacks in VANETs. The proposed approach leverages the signal strength of the jammer to estimate the distance between the jammer and the receiver. Subsequently, a less complex receiver. Subsequently, a less complex algorithm is introduced to localize the jammer and redirect vehicles away from the routes being exploited by the attacker.

III. LITERATURE REVIEW

L. Wei, J. Cui, Y. Xu, J. Cheng and H. Zhong et.al. addresses the importance of Vehicular Ad Hoc Networks (VANETs) in enhancing traffic safety and driving convenience due to advancements in wireless communication technology and the increasing number of automobiles. They identify the need for a Conditional-Privacy-Preserving Authentication (CPPA) scheme in VANETs, given their vulnerability and security requirements. Traditional CPPA schemes suffer from two shortcomings: insufficiently low communication/storage overhead for ultra-low transmission delay requirements of traffic emergency messages and neglect of system secret key (SSK) updates stored in tamper-proof devices, increasing the risk of SSK breaches [1]. To address these issues, the authors propose a CPPA signature scheme based on elliptic curve cryptography, ensuring message recovery and reduced communication overhead. They also introduce an SSK updating algorithm using Shamir's secret sharing and secure The review analyzes existing research contributions, highlighting their strengths, limitations, and potential areas for improvement. It synthesizes insights from different studies to identify common themes, emerging trends, and unresolved issues in the domain of VANET security, particularly concerning traffic emergency message authentication.

Dapeng Wu et.al addresses an energy-efficient data forwarding strategy (EDFS) aimed at addressing critical challenges in Wireless Body Area Networks (WBANs), particularly in the context of healthcare applications. These networks rely on body sensors with limited energy resources, making efficient energy management crucial to mitigate performance issues like latency and energy efficiency degradation. EDFS employs compressed sensing to reduce the size of transmitted physiological data and optimizes relay sensor selection by considering factors such as remaining energy levels, sampling frequency, and sensor importance. This approach enhances energy efficiency and network reliability while effectively adapting to dynamic WBAN topologies [2]. WBANs, a specialized subset of Wireless Sensor Networks, have garnered significant attention due to their capacity to collect diverse physiological data from wearable or implantable sensors, encompassing parameters like temperature, pulse, blood oxygen levels, blood pressure, electrocardiogram (ECG), and electroencephalogram, making them invaluable in the fields of biochemistry and healthcare. Given the resource-constrained nature of WBAN devices and the heterogeneous characteristics of sensor nodes, optimizing energy consumption during data forwarding becomes paramount for prolonging network lifetime and ensuring reliable data delivery.

Zongtao,Duan,Jabar Mahmood et.al. addresses the critical role of Vehicular Ad Hoc Networks (VANETs) in the autonomous vehicle industry, highlighting the escalating security threats accompanying advancements in VANET technology. They identify vulnerabilities in Xu et al.'s three-factor (3F) authentication scheme, revealing its susceptibility to dishonest Roadside Units (RSUs) bypassing the Trusted Authority (TA) and initiating unauthorized sessions with On-Board Units (OBUs). In response, Duan et al. propose a novel 3F authentication scheme called TFPPASV, designed to thwart RSU attempts at bypassing the TA while safeguarding user privacy [3]. Their scheme is tailored to meet the security and performance requirements of VANETs and is subjected to rigorous formal security analysis using BAN-Logic, alongside informal discussions of its security features. Additionally, the authors compare TFPPASV's security and performance against other recent schemes. As VANETs gain popularity for their potential to enhance road safety and enable autonomous vehicles, this research underscores the need for robust security measures within this dynamic

network structure, crucial for the future of transportation systems.

Chao Lin et al. address the challenges of security and privacy in Vehicular Ad-hoc Networks (VANETs), which have the potential to enhance driver safety and traffic management efficiency through real-time traffic information sharing among vehicles. They highlight the limitations of existing conditional privacy-preserving authentication (CPPA) protocols, particularly in the context of VANET deployment. To tackle these issues, the authors propose a novel blockchain-based CPPA (BCPPA) protocol, leveraging Ethereum as a public blockchain, to facilitate secure communication in VANETs [4]. This innovative solution incorporates a key derivation algorithm, reducing the burden of storing numerous private keys for participating vehicles. To enhance verification efficiency, their BCPPA supports batch verification with modified ECDSA or alternative PKI-based signatures. Additionally, the authors outline the security requirements met by their protocol and demonstrate its feasibility through implementation on the Ethereum test network (Rinkeby) and simulations using Vanet MobiSim and NS-2, achieving millisecond-level response times.

Jing Zhang; Jie Cui, et.al. enhancing security and privacy in Vehicular Ad-hoc Networks (VANETs) by addressing the limitations of existing identity-based vehicular communication protocols. Unlike conventional methods reliant on tamper-proof devices (TPDs), this novel protocol leverages the Chinese remainder theorem (CRT) to achieve conditional privacy-preserving authentication without the need for pre-loaded master keys on vehicles' TPDs. This dynamic CRT-based approach facilitates the generation and dissemination of group keys by trusted authorities (TAs), mitigating side-channel attacks and bolstering overall system security [5]. Importantly, it circumvents resource-intensive operations like bilinear pairing and map-to-point hashing during authentication, resulting in faster verification, even with an increasing number of signatures. Rigorous security analysis supports its resilience under the random oracle model, while performance analysis highlights its efficiency in reducing computational and communication overheads.

Zheng, Z., Zhang, Y., and Dai.H,et.al. addresses Vehicular ad hoc Networks (VANETs) are an emerging technology that plays a crucial role in the Intelligent Transport System. VANETs consist of smart vehicles and roadside infrastructure that communicate through open access wireless networks. However, as the number of vehicles continues to grow rapidly, VANETs become large-scale, dynamic, and heterogeneous, making them vulnerable to attacks that can jeopardize vehicular communication and endanger lives. To address this, VANETs must prioritize secure communication by implementing robust privacy-preserving and authentication mechanisms [6]. Additionally, efficiency is a significant concern in VANETs. While there have been numerous studies on privacy and security in VANETs, none have taken a holistic approach to these issues. In this paper, we provide a comprehensive background overview of VANETs and discuss various potential attacks. We classify privacy and authentication schemes into four major groups, considering their security mechanisms, requirements, strengths, limitations, attacks countermeasures, and performance and control measures.

G. Dubosarskii,S. Primak,et.al. addresses the field of anti-jamming games has gained considerable attention, but there is a dearth of publications specifically focusing on vehicular ad hoc networks (VANETs). To address this research gap, we developed a VANET anti-jamming game that incorporates a realistic driving model. Moreover, we introduced a quadratic power function in both the vehicle and jammer utility functions, thereby enhancing the realism of the game model. By utilizing mathematical methods, we derived the Nash equilibrium based on the system parameters for both single-channel and multi-channel scenarios [7]. Given that the network parameters are often unknown, we also compared the performance of several reinforcement learning algorithms that can iteratively converge to the analytically predicted Nash equilibrium without any prior knowledge of the environment in both static and dynamic scenarios.

S. Wang,C. Chu,et.al. addresses that jamming attacks have the potential to cause significant harm to Wireless Sensor Networks (WSNs). When a

jamming attack occurs, it is crucial to quickly determine the location of the jammer. This information is essential in order to develop effective countermeasures to mitigate the impact of the jamming. In this research paper, we propose a geometric covering method for jammer localization, which aims to minimize energy consumption. Additionally, we propose a compensating method that utilizes the power of the jamming signal received by the boundary nodes to reduce estimation errors in the jamming area [8]. Finally, we conduct localization by extracting the minimum covering circle of the compensated victim area. Through simulations, we evaluate the accuracy of our localization method considering factors such as node density, jamming region, and radius. The results demonstrate that our proposed method achieves both high precision and low energy consumption.

T. H. Aldhyani,H. Alkahtani,et.al. addresss the automotive industry has experienced a significant transformation due to the rapid advancement of technology. This progress has greatly impacted the way vehicles operate, with a shift towards software-controlled technologies and improved network communication. However, the autonomous vehicle network still faces cyber security vulnerabilities, primarily stemming from the intricate nature of data and traffic behaviors that can be exploited by unauthorized individuals. Detecting message attacks within the controller area network (CAN) poses a major challenge that needs to be addressed [9]. To tackle this issue, a high-performance system utilizing artificial intelligence techniques has been developed to safeguard the vehicle network from cyber threats. By leveraging deep learning approaches, the system effectively protects autonomous vehicles from intrusions. To validate its efficacy, the proposed security system underwent testing using a real dataset from an automatic vehicle network, encompassing various attack types and benign packets. The dataset underwent preprocessing to convert categorical data into numerical format. Subsequently, the convolution neural network (CNN) and a hybrid network combining CNN and long short-term memory (CNN-LSTM) models were employed to identify attack messages. The results demonstrated exceptional performance, as evidenced by high precision, recall, F1 score, and accuracy metrics.

Cui,Zhang, Zhong, Zhang ,Liu,et.al. addresses the challenges of securing group communication in Vehicular Ad hoc Networks (VANETs) through existing conditional anonymous authentication protocols include dynamically updating membership in a domain and preserving the privacy of vehicle users. This article presents a sophisticated solution to these challenges by introducing a new conditional privacy-preserving authentication protocol with dynamic membership for VANETs, based on the Chinese Remainder Theorem (CRT). In this protocol, a trusted authority utilizes the CRT to securely distribute a domain key to authorized vehicles within the same domain. Each vehicle in the domain can obtain the domain key by performing a single modulo division operation when the domain key needs to be updated. The review surveys existing research efforts and proposed authentication systems designed specifically for car networks, focusing on their capabilities in providing conditional privacy protection and their suitability for deployment in a multi-cloud environment [10]. It analyzes various authentication mechanisms, encryption techniques, and access control protocols employed to mitigate security risks and preserve user privacy in car-to-car and car-to-cloud communications. Unlike previous works in this field, our proposed protocol not only achieves message authentication, anonymity, and conditional privacy preservation, but also provides forward security and backward security for vehicles. Theoretical analysis and experimental simulations confirm that the proposed protocol is both provably secure and highly feasible.

G.Kasturi,A. Jain,J.Singh,et.al. addresses the jamming attacks that disrupt communication capabilities are becoming a critical concern in wireless networks. One of the main challenges is detecting reactive jammers who only target the network when legitimate communication is taking place. To address this issue, we propose a new framework for reactive jamming detection using external radio-frequency (RF) sensors. The review

also discusses challenges and limitations associated with RF jamming detection using machine learning, including data scarcity, feature selection, and model generalization across different jamming scenarios and environmental conditions [11]. This solution relies on two key components: a novel underdetermined blind source separation (UBSS) method that separates the jamming temporal profile from the network nodes' transmission profiles, and a new jamming detection technique called all-versus-one transfer entropy (AvOTE) based on causal inference.

M. Abdollahi, K. Malekinasab, W. Tu,M. Bag-Mohammadi,et.al. addresses the communication quality of wireless networks can be severely compromised by an active jammer. This is particularly problematic because all wireless nodes have unrestricted access to the shared media, which means that the adverse effects of jamming are amplified by the retransmission attempts made by affected devices. In heterogeneous wireless environments such as the Internet of Things (IoT), it is crucial to swiftly and accurately detect the presence of a jammer. To address this, we propose a local, straightforward, and numerical metric called the number of jammed slots (NJS) [12]. This metric enables us to rapidly identify the presence of a jammer and determine the affected nodes at the software level in broadcast networks. The calculation of NJS is carried out by a central node that periodically gathers the MAC-layer statuses of all wireless nodes. Our simulation results indicate that NJS outperforms existing detection methods in terms of accuracy and precision.

H.Pirayesh, P. K. Sangdeh, S. Zhang, Q. Yan,et.al. addresses the current intelligent transportation systems that rely on IEEE 802.11p for data collection and exchange face a significant vulnerability to jamming attacks. Although IEEE 802.11p offers low-latency communication, it lacks a practical countermeasure technique at the PHY-layer to combat jamming attacks. This paper introduces Jamming Bird, a novel receiver design that effectively withstands constant jamming attacks. Jamming Bird incorporates two MIMO-based techniques: a jamming-resistant synchronizer and a jamming suppressor. Together, these modules enable Jamming Bird to detect, synchronize, and recover desired signals even in the presence of jamming attacks, regardless of the PHY-layer technology used by the jammers. The review surveys existing research and proposed solutions tailored to mitigate the impact of jamming attacks on VANETs. It scrutinizes various approaches, including signal strength analysis, frequency hopping techniques, and adaptive routing protocols, to gauge their effectiveness in thwarting jamming attempts and sustaining communication integrity in VANETs [13].To evaluate its performance, Jamming Bird has been implemented on a vehicular test bed, and extensive experiments have been conducted in various vehicular scenarios, including parking lots (0-15 mph), local traffic areas (25-45 mph), and highways (60-70 mph). The results of these experiments demonstrate that while conventional 802.11p-based receivers experience an 86.7% degradation in throughput due to jamming attacks, Jamming Bird maintains an average throughput of 83.0%. Furthermore, the experimental results indicate that Jamming Bird can tolerate jamming signals with 25 dB stronger power than the desired signals.

V. K. Kukkala, S. V. Thiruloga,S. Pasricha,et.al. addresses the advent of autonomous vehicles is imminent and will bring about a transformation in transportation safety and convenience. These vehicles will be interconnected with various external systems and employ sophisticated embedded systems to perceive their surroundings and make intelligent decisions. However, this increased connectivity exposes these vehicles to a range of cyber-attacks that can have devastating consequences. Incidents of attacks on automotive systems are already on the rise in today's vehicles and are expected to become more commonplace in future autonomous vehicles. The review surveys existing research and industry initiatives aimed at enhancing cybersecurity in AVs, focusing on key areas such as threat modeling, risk assessment, intrusion detection, and secure communication protocols [14]. It evaluates the effectiveness of different approaches and identifies gaps in current cybersecurity strategies for AVs Hence, there is a pressing need to bolster cyber security in future autonomous vehicles. In this article, we delve into

major cyber-attacks on automotive systems over the past decade and present state-of-the-art solutions that leverage artificial intelligence (AI).

Y. S. Kim, F. Mokaya, E. Chen, and P. Tague,et.al. addresses the localization of wireless sensors under jamming attacks reveals a multifaceted landscape marked by diverse methodologies and strategies. Researchers have explored various techniques, including signal strength-based methods, time of arrival (TOA), time difference of arrival (TDOA), and angle of arrival (AOA) approaches, among others, to mitigate the impact of jamming on sensor localization accuracy [15]. Studies highlight the challenges posed by different jamming characteristics such as power levels, frequency ranges, and modulation schemes, and propose innovative solutions such as cooperative localization, robust algorithms, and hardware enhancements to enhance resilience against jamming threats. By synthesizing insights from diverse studies, the review identifies common limitations and challenges encountered in jamming localization approaches, including susceptibility to environmental conditions, scalability issues, and computational complexity. It also explores advancements in machine learning and signal processing techniques for enhancing localization resilience under jamming. Additionally, investigations delve into the theoretical foundations, practical implementations, and performance evaluations of these techniques across different scenarios and environments, aiming to provide insights and guidelines for designing robust and efficient localization systems in the presence of jamming interference.

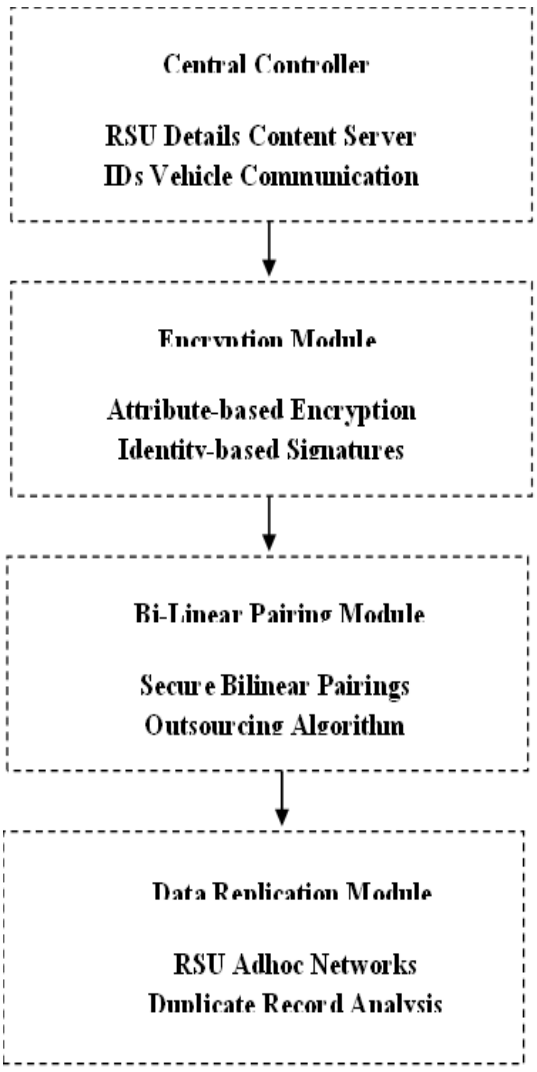
I. K. Azogu, M. T. Ferreira, J. A. Larcom, and H. Liu, et.al proposed novel anti-jamming strategy for Vehicular Ad Hoc Networks (VANETs) focuses on metrics-directed security defense. The strategy employs a comprehensive literature review to identify key metrics crucial for VANET security enhancement. Through this approach, it aims to mitigate the impact of jamming attacks, a significant threat to VANET communication reliability and safety[16]. By analyzing existing literature, the strategy aims to understand the vulnerabilities and shortcomings of current anti-jamming techniques while proposing innovative solutions tailored to specific metrics. This metrics-directed approach enhances the effectiveness and efficiency of security defense mechanisms in VANETs, ensuring robustness against jamming attacks while preserving network performance and reliability. Through empirical evaluation and simulation, this strategy seeks to validate its effectiveness and practical applicability, contributing to the advancement of VANET security protocols and fostering more resilient vehicular communication systems.

AUTHOR	ISSUE IDENTIFIED	METHOD / ALGORITHM	PARAMETERS
D. Kosmanos, A. Argyriou, and L. Maglaras,et.al	The objective is to determine the relative velocity of a mobile vehicle that disrupts RF communication between a transmitter and receiver pair.	Radio frequency (RF), Angle of projection(AOP)	Signal characteristics, geospatial information, Doppler shift, and signal strength
D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. J. Aparicio-Navarro, A. Argyriou, and H. Janicke, et.al	The objective is to design an intrusion detection system that utilizes machine learning techniques in order to safeguard electric vehicles from spoofing attacks.	K-NN, RaFo	CAN Bus Anomalies,Vehicle Network Traffic Analysis,Message Authentication and Validation.
L. Rajesh, K. B. Bagan, P. T. Sankar, and V. Suchitra,et.al	The implementation of q-learning analysis has enabled the utilization of unmanned aerial vehicles (UAVs) in monitoring communication status.	Q-learning analysis	Throughput and Data Transmission Efficiency,Jamming Detection and Adaptation,Network Resilience and Reliability.
D. Kosmanos, D. Karagiannis, A. Argyriou, S. Lalis, and L. Maglaras,et.al	In order to implement supervised learning, specifically k-nearest neighbours (KNN) and random forest (RAFO), for the purpose of creating a detection method, we will utilize the differences in relative speed as the primary factor.	K-NN, RaFo	Doppler Shift,Geos,patial Integration,Signal Processing
G. B. Santhi and D. Sheela,et.al	In order to safeguard the communication of vehicles, a novel index-based voting technique is being devised to counteract hybrid jamming attacks.	IBVA	Network Reliability,Cooperative Voting Dynamics
J. Fan, T. Liang, T. Wang, and J. Liu,et.al.	To achieve the localization of the jammer, it is essential to deploy the geometry of the jammed nodes and boundary nodes.	RJSS	Signal Strength,Time of Arrival,Frequency Analysis
S. Wang and C. Chu,et.al.	The jamming strength can be effectively employed through a geometric covering approach to accurately determine the location of the jammer.	GJL	Distance Comprehension,Geometric Coverage,Computational Efficiency
W. Aldosari and M. Zohdy,et.al	In a scenario involving a moving jammer attack, the process of selecting a boundary node can be achieved by calculating the	Extended Kalman filter	Signal-to-Noise-Ratio (SNR)Estimation,Extended Kalman Filter (EKF) Performance,Selection of Boundary Nodes

	node's maximum reachable sensing range.		
T. Zhang, X. Ji, Z. Zhuang, and W. Xu,et.al.	To address the issue of mobile jamming attacks on advanced metering infrastructure (AMI), we introduce a localization system that provides enhanced protection.	DiffLSQ, LimTrack	Localization Accuracy,Real-time Detection and Response,Robustness in Dynamic Environments.
I. K. Azogu, M. T. Ferreira, J. A. Larcom, and H. Liu,et.al.	To offer a novel solution to address the issue of jamming in VANET infrastructure by proposing a hidden anti-jamming strategy.	Channel Surfing and Hideaway	Metric-Based Attack Detection,Adaptability to Varying Attack Scenarios,Communication Performance Metrics

TABLE FOR RELATED W

IV. BLOCK DIAGRAM



ORKS

Figure 1. Block Diagram

Proposed System

The proposed approach uses Identity-Based Online/Offline Digital Signature (IBOOS) for secure data transmission in Cluster-based Wireless Sensor Networks (CWSN). Leveraging clustering, we introduce two Secure and Efficient Data Transmission (SET) protocols to enhance network performance. IBOOS builds upon the lightweight CP-ABE scheme, streamlining the architecture and reducing reliance on trusted authorities. By encrypting user information with our proposed method and uploading it as ciphertext to the VC, we minimize communication overhead and increase efficiency. Our system features a central controller housing content server, RSU (ROAD SIDE UNIT) details, and vehicle information. Multiple control servers can be generated, each displaying available content server IDs in the respective RSU form. Vehicles' data replication occurs at the nearest RSU, optimizing data distribution and accessibility in vehicular networks while maintaining security and efficiency.

Module Description

Central Controller

The central controller module manages RSU details, available content server IDs, and facilitates communication with the nearest vehicle through RSUs. Serving as the central hub, it organizes RSUs under content servers, displaying RSU and location IDs. Vehicle data replication is also coordinated by the server. Software-defined networks allow for programmable configuration, enabling network administrators to script SDN programs for configuring, managing, securing, and optimizing network resources automatically. Open and VANET methods are essential for this purpose, ensuring flexibility and avoiding server lock-in through open APIs. This abstraction enables hardware agnosticism, akin to personal computers, eliminating concerns about hardware compatibility. In summary, the central controller module efficiently manages RSU and content server details, coordinates vehicle communication, and leverages software-defined networks for streamlined network administration and resource allocation.

Encryption

The CP-ABE based IBOOS scheme assigns unique attributes to each user, each corresponding to a private key. An encryption strategy is devised by the encryptor, allowing only users with attributes that match the strategy to decrypt the ciphertext. A lightweight CP-ABE scheme is proposed for mobile cloud-assisted cyber-physical systems, featuring three key algorithms:

1. Key Management: This algorithm is responsible for distributing public parameters and securely maintaining a master secret key for the entire system.
2. Encryption: This process generates ciphertext using the public parameters, data, and access policy. The ciphertext is then transmitted to the cloud for storage.
3. Decryption: This algorithm retrieves the original data from the ciphertext using the master secret key and a set of attributes that comply with the decryption policy. Users lacking the required attributes specified in the decryption policy are unable to decrypt the ciphertext.

Bilinear Pairing

The bilinear pairing refers to a mathematical operation that combines elements from two distinct groups and produces a result in a third group. Bilinear pairings are often used in cryptographic protocols within VANETs to enable secure communication and authentication between vehicles. An efficient and secure outsourcing algorithm for bilinear pairings is done. This algorithm is used as a subroutine to achieve outsource-secure identity-based encryptions and signatures.

Data Replication

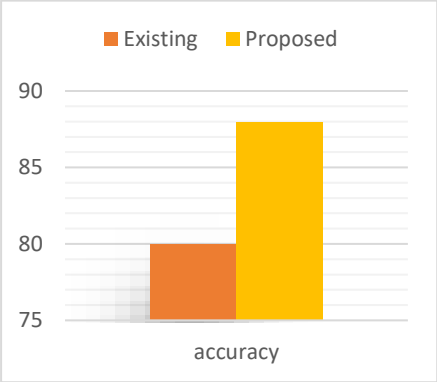
In this module, data replication becomes feasible with enhanced precision in RSUs within the vehicle ad hoc network. Each RSU possesses its ad hoc model, facilitating the identification and analysis of duplicate records. The system detects matched records across different RSUs, initiating the replication process. Each vehicle ad hoc network within the RSU unit manages its specific vehicle ad hoc network. The Database Replication module enables data importation from existing databases. Moreover, it supports complex mappings across

multiple table joins. This feature enhances the system's capability to replicate data effectively, ensuring synchronization across RSUs and vehicle ad hoc networks. Through meticulous analysis and management at both the RSU and vehicle ad hoc network levels, the replication process maintains data integrity and consistency throughout the network infrastructure.

V. Result Analysis

The proposed dynamic routing system demonstrates a markedly higher level of accuracy in comparison to the current static routing infrastructure. Boasting an impressive 88% accuracy rate, it represents a notable advancement in addressing identified challenges and enhancing the operational capabilities of Wireless Sensor Networks. This significant improvement highlights the efficacy of the proposed solution in facilitating data transmission within wireless sensor networks, emphasizing both safety and efficiency enhancements.

Algorithm	Accuracy
Existing	80
Proposed	88



Conclusion

Vehicular Ad Hoc Networks (VANETs) provide a significant advantage in enhancing road safety, offering features like collision avoidance systems, emergency vehicle notifications, and adaptive cruise control. These networks have the potential to reduce accidents and save lives by enabling real-time data sharing among vehicles. This sharing of crucial information about traffic conditions, accidents, and road hazards empowers drivers and autonomous systems to make more informed and safer decisions. VANETs represent a technological leap, allowing vehicles to interact with each other and with infrastructure elements, ushering in a new era of vehicle communication. VANETs go beyond safety benefits; they hold the promise of minimizing traffic congestion and improving overall traffic flow. Through applications that optimize traffic signal timings and reroute vehicles to less congested paths, VANETs aim to revolutionize transportation.

References

[1] L. Wei, J. Cui, Y. Xu, J. Cheng and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs", IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1681-1695, 2021.

[2] Dapeng Wu "An Energy-Efficient Data Forwarding Strategy for Heterogeneous WBANs",21 September 2016,IEEE,10.1109/ACCESS.2016.2611820.

[3] Zongtao Duan,Jabar Mahmood ,"TFPPASV: A Three-Factor Privacy Preserving Authentication Scheme for VANET",Revised 6 August 2022; Accepted 12 August 2022; Published 30 September 2022.

[4] Chao Lin; Debiao He,"BCPPA: “A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks",: IEEE Transactions on Intelligent Transportation Systems.

[5] Jing Zhang; Jie Cui,"PA-CRT: “Chinese Remainder Theorem Based Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks", IEEE Transactions on Dependable and Secure Computing

[6] Zheng, Z., Zhang, Y., and Dai, H. (2019). "A survey on blockchain and the internet of things". IEEE Journal of Internet of Things, 6(5), 8076–8094.

[7] Dubosarskii and S. Primak, ‘‘Jamming and anti-jamming strategies of mobile vehicles,’’ Electronics, vol. 10, no. 22, p. 2772, Nov. 2021.

[8] Wang and C. Chu, ‘‘Geometry-covering jammer localization based on distance comprehension in wireless sensor networks,’’ 2015,arXiv:1512.06468.

[9] T. H. Aldhyani and H. Alkahtani, ‘‘Attacks to automatous vehicles: A deep learning

algorithm for cybersecurity,'' Sensors, vol. 22, no. 1, p. 360, 2022.

[10] Cui (2020), Zhang (X.), Zhong (2020), Zhang (2020), & Liu (2020)."Comprehensive conditional privacy protection authenticatIon system for safe car networks in a multi-cloud setting".

[11] G.Kasturi, A. Jain, and J. Singh, ''Detection and classification of radio frequency jamming attacks using machine learning,'' J. Wireless Mob. Netw. Ubiquitous Comput. Dependable Appl., vol. 11, no. 4, pp. 49–62, 2020.

[12] M. Abdollahi, K. Malekinasab, W. Tu, and M. Bag-Mohammadi, ''An efficient metric for physical-layer jammer detection in Internet of Things networks,'' in Proc. IEEE 46th Conf. Local Comput. Netw. (LCN), Oct. 2021,pp. 209–216.

[13] H. Pirayesh, P. K. Sangdeh, S. Zhang, Q. Yan, and H. Zeng, ''Jamming-Bird: Jamming-resilient communications for vehicular ad hoc networks,''in Proc. 18th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON),Jul. 2021, pp. 1–9.

[14] V. K. Kukkala, S. V. Thiruloga, and S. Pasricha, ''Roadmap for cyber security in autonomous vehicles,'' IEEE Consum. Electron. Mag., vol. 11,no. 6, pp. 13–23, Nov. 2022.

[15] Y. S. Kim, F. Mokaya, E. Chen, and P. Tague, ''All your jammers belong to us—Localization of wireless sensors under jamming attack,'' in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp. 949–954.

[16] I. K. Azogu, M. T. Ferreira, J. A. Larcom, and H. Liu, ''A new anti-jamming strategy for VANET metrics-directed security defense,'' in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2013, pp. 1344–1349.