Secure Protocol for VANETs Communication

Manish Kumar
S.V. National Institute of Technology,
Surat, India
manishbhatti20@gmail.com

Shriniwas Patil
S.V. National Institute of Technology,
Surat, India
shriniwas1996@gmail.com

Keyur Parmar
S.V. National Institute of Technology,
Surat, India
keyur@coed.svnit.ac.in

***Abstract*—Vehicular ad hoc Networks (VANETs) are receiving great attention lately from academia and industries as well. So various research is going on covering different aspects of VANETs including security and safety of communication channels. One of the major challenges is preserving the privacy and security of vehicles while communicating with each other. Security becomes challenging when we have to trace the malicious nodes, in the network to punish or revoke malicious nodes, as we have to hide identity of sender during communication . In this article, we propose a secure authentication protocol for communication in VANETs that can achieve desired conditional privacy along with security during transmission of messages.**

***Index Terms*—VANETs, Privacy, Security, Authentication**

I. Introduction

The number of vehicles are increasing day by day, also the number of road accidents has been increasing. In one study [1], authors found that road accidents has increased at an alarming rate of 2.1% per year in last decade. Therefore, the need of automation to manage traffic and establish proactive warning system is inevitable in vehicles.

VANETs are a network of interconnected vehicles that can communicate over a channel. Network nodes can exchange the state of traffics, accident situations with other vehicles or traffic control centers which can help in modulating the traffic control in an optimized way. Therefore, VANETs try to reduce the human reliance on vehicle driving and facilitate proactive data and information sharing. The VANET model [2] comprises of two main components namely On Board Unit (OBU) and Road Side Unit (RSU).

OBUs are installed in vehicles to communicate or even perform some computations such as gathering information from sensors and radar in vehicle and process data to share with OBUs installed in other vehicles. RSUs works as access points to control the network. The OBU and RSU work together over wireless medium to form a VANETs infrastructure [3].

The need for fast communication makes VANETs vulnerable to security and privacy attacks especially if the communication medium is wireless. Therefore, preserving the authenticity, confidentiality, and integrity of transmitted and received packets remains a challenge in such networks. Attackers can also trace the location of any vehicle if appropriate privacy protocols are not employed.

Message authentication can be used to solve some of the challenges related to security. However, the privacy of vehicles transmitting the messages is also important as attackers can trace the location of the vehicle by exploiting the loopholes in implementation of privacy protocols. Another challenge is, we need conditional privacy as there is no way to punish the malicious vehicles without disclosing their identity to central authority.

There exists three kind of solutions for Conditional Privacy Preserving Authentication (CPPA), namely Public Key Infrastructure (PKI) based, identity (ID)-based and Zero-knowledge proof (ZKP) based. Shim [4], Zhang et al. [5] , Zhang et al. [6] have studied PKI based CPPA. Other solutions are ID based such as Raya and Hubaux [7] and Lin et al. [8]. PKI based [9] have challenges in key management and key revocation mechanism and ID based solution also suffers from problem such as intractability of revoking the vehicles' private key. Some solutions that are blockchain-based [10], [11], are also presented to overcome the challenges, but blockchain solutions are complex and not feasible [12]. Scalability is a challenge in blockchain solutions. Authors [13] have explored ZKP based security and privacy implementation but despite all the intense research going on in ZKP domain, a major challenge for ZKP based solutions [13], [14] is that they are always vulnerable to Man-in-the-Middle attack as no shared keys are used in ZKP solutions.

In this article, we devise a well versed model for VANETs that can preserve the privacy and security of vehicles over the course of whole communication with other entities in the model. We concentrate on conditional privacy instead of privacy because conditional privacy can help to punish the malicious nodes in network and malicious nodes can be removed from network. Therefore, we will have a trusted authority that can access the private information of the vehicles.

In the proposed protocol, we use cryptographic primitive such as digital signature and encryption algorithms to provide security for exchanged payload. The proposed protocol ensures that vehicles are not able to link the two messages from the same sender and prevent the sender from traceabilty attacks.

After the successful implementation of proposed protocol we are able to ensure that our protocol fulfill security requirements. The proposed protocol use encryption to enhance the performance along with security. The AES is used as the symmetric encryption algorithm and RSA is used for asymmetric encryption.

In this article, our contributions are as follows:

1) We present a comprehensive review of the state-of-the art literature to identify the challenges in VANET communication.

2) We proposed a secure protocol for VANET communication that provides untraceable authentication to the vehicles in the network.
3) We analyse the security strength and evaluate the performance of the proposed protocol for VANET communication.

The rest of the article is organised as follows. In section II, we discusses the background research and literature survey. Section III discusses the preliminaries related to the proposed secure protocol for VANET communication. In section IV, we discuss the security and privacy model and working of proposed secure model for VANET communication. In section V, we discuss strategies and methodology in terms of implementation of our protocol. In section VI, we presented results of implementation and analyse the security of the proposed secure protocol for VANET communication. In section VII, we conclude the article.

II. Related Work

The VANET has emerged from Intelligent Transport System (ITS). Toh [15] discussed car-to-car Mobile Ad hoc Network (MANET) and presented the concept of VANET. Author has shown that VANETs are going to be key part in developing ITS to provide traffic safety, navigation, and other applications. Hubaux et al. [16] identified the need of security and privacy in VANETs. Similarly, Zarki et al. [17] discussed the role and importance of implementing security and privacy in VANETs.

Raya and Hubbaux [7] proposed the concept of conditional privacy preservation. Authors presented a modified PKI model to implement anonymous certificates to preserve privacy of nodes. However, public-private key pair is required to be preloaded into the OBU and RSU in the initialisation phase for the modified PKI solution, i.e large amount of storage is required for OBUs. However, providing large amount of storage is not feasible for low storage device like OBUs. Another challenge with PKI based solutions was complexity while revoking certificates. Aslam and Zou [18] proposed an architecture that based on restricted certificates for each node in network which are easy to revoke if required. The architecture provided makes key assumption that VANETs area are isolated and independent of each other. However, that is not true in the case of VANETs as area under different RSUs can overlap with each other and transition from RSU to RSU must be considered.

Lu et al. [9] identified that providing anonymity is not sufficient for privacy and discussed the tracking attacks are still the possibility in anonymous authentication, and provide a number of location privacy protection measures as a supplement to anonymous authentication. Malicious vehicles in the network could track the activities of the targeted driver, based on the information provided for authentication.

Raya and Hubbaux [19] analysed the security of VANETs and studied the design challenges while implementing VANET solutions and proposed security protocol. However, the proposed security protocol does not provide privacy and robustness. Later, Raya et al. [20] overcame the privacy challenges using temporary pseudonyms and anonymity techniques but generating pseudonym creates storage and computation overhead on Certificate Authority (CA) as well as OBUs.

Lin et al. [21] and He et al. [22] proposed privacy-preserving solutions based on group signature and ID-based signature. However, malicious vehicles can also achieve anonymity, which makes it difficult for the trusted authority, such as the vehicle administration centres, to revoke their access after tracking them. A token-based non-interactive authentication scheme where every group has shared public key, is devised by Salem et al. [23] in which privacy is ensured by changing the set of public key of members frequently by using digital signature algorithm. Whyte et al. [24] presented a solution based on butterfly key expansion to generate pseudonym and certificates of those pseudonym to provide untraceability and privacy. However, butterfly key expansion fails to provide efficient key revocability. Therefore, the concept of conditional privacy preservation was coined to overcome the above challenges. Lin et al. [21] integrated the concept of group signature and ID-based signature to introduce a secure conditional privacy preserving protocol. Guo et al. [25] presented a security framework based on group signature. Boneh and Franklin [26] used bilinear pairings on elliptic curves to develop the efficient ID-based encryption scheme. Existing CPPA protocols for VANETs can be categorized into PKI based [7], [16], ID-based [4], [22] or ZKP based [13], [14].

With developments in domain of ZKP, researchers have tried to devise models and frameworks using ZKP, for preserving privacy while data sharing [14] and authentication [13]. However, ZKP based models face a challenge such as MITM attack, and it is challenging because with ZKP based solution we refrain to use key based cryptography which leads to possibility of MITM attack.

PKI based protocols suffers from challenges such as preloading keys or certificates and revocation. ID based protocols does not suffer from preloading keys or certificates and revocation challenges. However, they have other challenges such as intractability while revoking vehicle's certificate. Many models such as [5] and [6] further use batch verification in order to improve the performance.

The above challenges still exist in blockchain based models [27]. Mejri et al. [3] has provided a comprehensive survey of how blockchain can be useful for creating various security solutions for VANETs. Since, the introduction of bitcoin, the blockchain technology has emerged as viable solution for challenges related to security, privacy and trust. Blockchain has been used to overcome the challenges of security and privacy in VANET applications. Authors [9] integrate the blockchain and cryptographic primitives to provide privacy-preserving authentication. Similarly, Patel et al. [28], Zheng et al. [27], and Li et al. [29] proposed models for security and privacy based on ECC (Elliptic Curve Cryptography), PoW (Proof of Work), and merkle tree based authentication, respectively. Wagner et al. [12] discussed the PoW and full blockchain validation is not possible for VANET solutions. Although, many articles such as [30] proposed the models

TABLE I
COMPARISON OF DIFFERENT PERMISSIONED BLOCKCHAIN BASED ELECTRONIC HEALTH RECORD SHARING MECHANISMS

Reference	Technology	Advantages	Disadvantages
Raya and Hubaux, 2005 [7]	PKI	Provided a modified PKI model to implement anonymous certificates to preserve privacy	Private or public key pair are to be preloaded and key revocation problem
Aslam and Zou, 2009 [18]	PKI	Based on restricted certificate which are easy to revoke if needed	Does not account the transition of vehicle from one RSU to another
Raya et al., 2007 [19]	PKI	Overcome privacy issues using pseudonyms	Key revocation problem and not scalable
Lin et al., 2007 [21]	Group signature and ID based	Along with privacy and security, also provide traceability in case of dispute events	Any malicious vehicle can also achieve anonymity
He et al., 2015 [22]	ID based	Provide security and privacy with enhanced performance	Intractability of revoking node's key
Salem et al., 2010 [23]	Group signature	Privacy is ensured by changing the set of public key of members frequently by using DSA	Does not provide message authentication
Whyte et al., 2013 [24]	PKI	Use butterfly key expansion to generate pseudonym and pseudonym certificates to provide untraceability and privacy	Fails to provide efficient key revocability
Gabay et al., 2020 [13]	ZKP	Provide privacy preserving authentication using computation verifiability	Possibility of man-in-the-middle attack
He et al., 2021 [10]	Blockchain based PKI	Dynamic key generation algorithm to generate pseudonym to provide privacy preserving authentication	Key generation algorithm has private key generation vulnerability

based on PoW. Authors [31] uses batch verification and aggregation to reduce the cost of computation and uses two layers of blockchain to protect privacy. Blockchain is also used in reputation based networks to provide immutability to reputation data [32]. The reputation and incentive can be used to improve trust and security [11] by preventing spamming and denial-of-service attacks by limiting the power of a node. Despite all this blockchain based solution are complex and can be risky to be used in real time networks like VANETs.

The existing proposed mechanisms are not feasible in real time communication. Therefore, we propose a security protocol for VANET communication using primitive cryptographic techniques to provide security and achieve privacy-preserving authentication.

III. PRELIMINARIES

A. Public Key Encryption Algorithm

- **RSA**: Rivest-Shamir-Adleman (RSA) is the public key encryption. It is a block cipher that uses an asymmetric key pair i.e., a public key and a private key. The public key can be used to encrypt a message, and the private key can be used to decrypt it.

B. Symmetric key Algorithm

- **AES**: Advanced Encryption Standard (AES) is a symmetric key algorithm that is used to encrypt and decrypt data. AES is a block cipher, which means that it takes a block of data and encrypts it using a key. The key is then used to decrypt the data.

IV. PROPOSED PROTOCOL FOR VANETS COMMUNICATION

The proposed secure protocol for VANETs communication is illustrated in Figure 1. A brief description of each entity is as shown in Table III. The proposed protocol composes ten steps and divided into two phases as shown in sections IV-A and IV-B, respectively. The notations and their descriptions used in proposed protocol is shown in Table II.

TABLE II
NOTATIONS AND DESCRIPTIONS IN PROPOSED PROTOCOL

Notation	Description
C_{UID}	Payload created by encrypting UID and public key of V1 using public key of CA
(sk_{vi}, pk_{vi})	Vehicle's private/public key pair
(sk_{CA}, pk_{CA})	CA's private/public key pair
S_i	Symmetric key of vehicle i
M	Actual message
C_{M_1}	Payload created by encrypting actual message using S_1, to be sent from V_1 to V_2
C_{S_1}	Payload created by encrypting symmetric key of V_1 using pk_{CA}, to be sent from CA to V_1
C_{pv}	Payload created by encrypting public key of V_1 using pk_{CA}, to be sent from V_1 to V_2
C_{M_1}	Payload created by encrypting actual message using S_2, to be sent from CA to V_1

TABLE III
ENTITIES AND ROLES

Entities	Roles
Certificate Authority	Certificate Authority produces and manages digital certificates of OBUs and RSUs. The certificate authority stores the public key and symmetric key for all the vehicles along with UIDs of the vehicles.
Road Side Unit	Road Side Units are installed on roads to provide a local CA to connect with vehicles.
On Board Unit	Vehicles are installed with OBUs or over board Units which helps them to connect to RSUs and other OBUs.

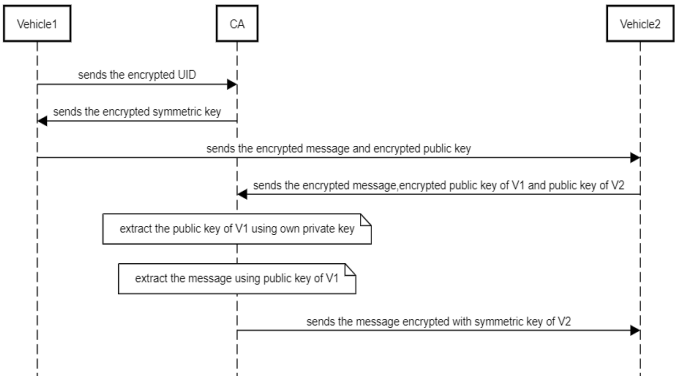

Fig. 1. Sequence diagram of secure protocol for VANET communication protocol

A. System Initialisation Phase

The system initialisation phase is further divided into eight steps.

1) Certificate authority and vehicle owners generate public-private key pair (pk_{CA}, sk_{CA}) and (pk_{v_i}, sk_{v_i}), respectively using RSA key generation algorithm.
2) The vehicle V_1 encrypts the UID and public key pk_{v_1} using public key of certificate authority pk_{CA}. Vehicle V_1 sends the C_{UID} to the certificate authority.

$$C_{UID} = Encr_{pk_{CA}}(UID \mid\mid pk_{v_1})$$

$$V_1 \xrightarrow{C_{UID}} CA$$

3) Certificate authority verifies UID with authorities and law enforcement agencies. If verification is successful an entry is created for V_1 that maps UID to pk_{v_1} along with symmetric key S_1, which is unique for each vehicle and generated using AES symmetric key algorithm.
4) Certificate authority encrypts S_1 using public key pk_{v_1} of vehicle V_1. Certificate authority sends C_{S_1} to vehicle V_1.

$$C_{S_1} = Encr_{pk_{CA}}(S_1)$$

$$CA \xrightarrow{C_{S_1}} V_1$$

5) Vehicle V_1 decrypts C_{S_1} using secret key sk_{v_1} and extract the symmetric key S_1 and stores it.

$$S_1 = Decr_{sk_{V_1}}(C_{S_1})$$

B. Communication Phase

6) To send message *M* from vehicle V_1 to V_2, V_1 encrypts message *M* using symmetric key S_1 and also encrypt public key pk_{v_1} using public key of CA so that only CA could fetch public key of V_1.

$$C_{M_1} = Encr_{S_1}(M)$$

$$C_{pv} = Encr_{pk_{CA}}(pk_{V1})$$

7) V_1 sends the C_{M_1} and C_{pv} to vehicle V_2.

$$V_1 \xrightarrow{C_{M_1}, C_{pv}} V_2$$

8) Vehicle V_2 sends C_{M_1}, C_{pv} and public key pk_{V_2} to certificate authority.

$$V_2 \xrightarrow{C_{M_1}, C_{pv}, pk_{V_2}} CA$$

9) Certificate authority first decrypt C_{pv} to retreive the public key of sender vehicle i.e pk_{V_1} and retrieves symmetric key S_1 corresponding to pk_{V_1} and decrypts C_{M_1} and encrypts the decrypted message M using S_2.

$$M = Decr_{S_1}(C_{M_1})$$

$$C_{M_2} = Encr_{S_2}(M)$$

10) The certificate authority sends C_{M_2} to th e vehicle V_2 and vehicle V_2 gets the message by decrypting C_{M_2} using private key sk_{V_2}

$$CA \xrightarrow{C_{M_2}} V_2$$

$$M = Decr_{sk_{V_2}}(C_{M_2})$$

V. Methodology

To implement our protocol, we need a technology that support real time communication between nodes. Therefore, we use JavaScript. Details on JavaScript are given in section V-A.

A. JavaScript and its Libraries

We use two JavaScript libraries namely PubNub and CryptoJS to implement proposed secure protocol for VANET communication.

B. PubNub

PubNub is used to work with real-time data. PubNub provides a great feature called channels, through which communication can take place between two differnet nodes. PubNub uses publish and subscribe model. Node receiving the message should be subscribed to a channel and node sending the message put the message on channel.

C. CryptoJS

CryptoJS is a JavaScript library that provides cryptographic functionality. CryptoJS is primarily used for two purposes: encrypting data and generating message digests.

D. Implementation Details

To implement proposed secure protocol for VANET communication, we take up a simple model that consist of three nodes as below:

- Vehicle sending message (V_1)
- Vehicle receiving message (V_2)
- CA

We have created following three channels as shown in Figure 2.

- C_1: To communicate between V_1 and CA
- C_2: To communicate between V_2 and CA
- X: To communicate between V_1 and V_2.

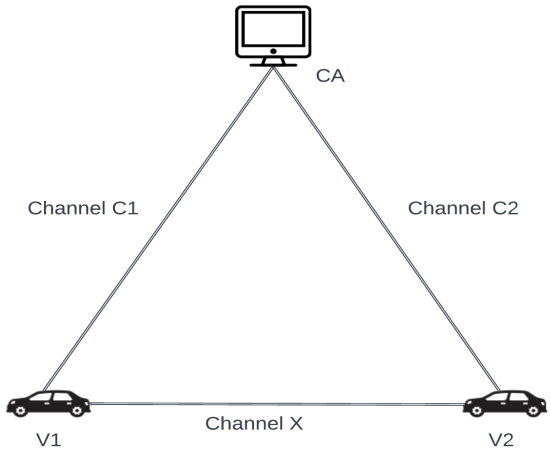

Fig. 2. Channel allocation for communication

VI. Results and Analysis

A. Implementation Result

To implement our model, we have created three nodes representing V_1, V_2 and CA. V_1 will first register itself by sending his UID and public key and receive a symmetric key for future use in encrypting his messages before sending to V_2. At this point V_1 is ready to send message and when required V_1 can send message by entering the message in text box as shown in Figure 3.

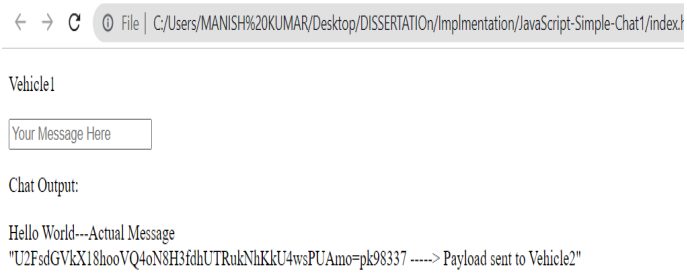

Fig. 3. Vehicle V_1 sending message

Actual message and message payload after encryption with symmetric key of V_1 concatenated with public key of V_1, are shown in Figure 4.

Payload received from V_1, payload sent to CA, payload (actual message encrypted by V_2's symmetric key) received from CA, and actual message after decryption by V_2, all are shown on the screen of V_2 as shown in Figure 4.

Similarly, payload received from V_2, decrypted actual message and encrypted message payload to be sent to V_2, are all shown in Figure 5.

B. Security Analysis

The proposed model for VANET communication is easy to implement, practical and scalable. We analyse the proposed

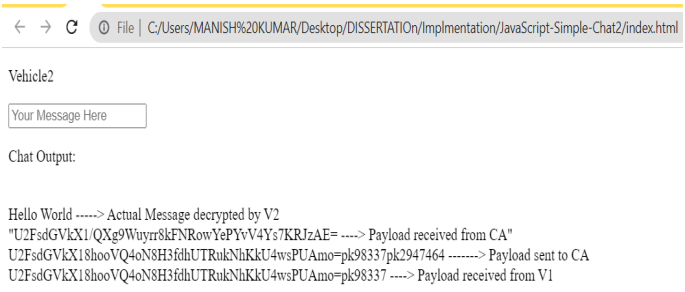

Fig. 4. Vehicle V_2 receive payload and sending to CA

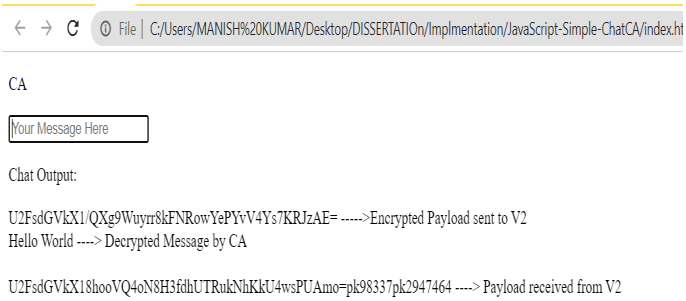

Fig. 5. CA receive payload and sending to vehicle V_2

security protocol for VANET communication with security perspective below.

Message Authentication: Security of our protocol mechanism is such that, attacker cannot send a legitimate message to any other vehicle in network. As the public key of the sender is first verified by CA, and message and public key are encrypted at each stage of the transition of the message.

Integrity: The receiver can verify the message's legitimacy and integrity through CA and receivers' identity can also be verified by the CA.

Message Confidentiality: In the proposed protocol, the message is encrypted using symmetric key by the vehicle sending message and certificate authority to achieve the confidentiality of the message. .

Conditional Privacy Preservation: No one is able to detect the identity of the sender of the message apart from CA. Therefore, conditional privacy is achieved.

Unlinkability: To send the message M, the car will encrypt the message with its symmetric key and public key it sends is also encrypted using public key of CA. Hence, there is is no way for a vehicle to link two messages whether they are from same sender or not.

C. Performance Analysis

There are few softwares for simulation of VANETs, specially for those which use cryptographic primitives as security measures. Therefore, we have implemented a protocol using JavaScript to check the the capability and feasibility of our protocol. Following are some performance result taken out of our implementation:

1) RSA key generation takes `90ms` to generate public-private key.
2) AES encryption takes `56ms` to encrypt the message.
3) To send message from Vehicle to CA takes approximately `132ms` on an average.
4) To send message from vehicle to vehicle take approximately `78ms` on an average.

VII. Conclusions and Future Works

In this article, we propose a security protocol for VANET communication. To provide secure communication between vehicles and RSUs, we need secure protocol in VANET. The proposd secure protocol for VANET communication uses CA to provide trust in the system. The protocol is secure and reliable to communicate in VANET. In addition, the protocol protects privacy of vehicles in the network. In future, we may use the blockchain technology to make the system transparent.

Acknowledgement

This research was a part of the project "Design and Analysis of Secure and Efficient Smart Contracts Using Blockchain Technology". It was partially supported by the SEED Money/Research Grant of the author, Dr. Keyur Parmar, Department of Computer Science and Engineering, S. V. National Institute of Technology (NIT), Surat, India.

References

[1] M. Ruikar, "National statistics of road traffic accidents in india," *Journal of Orthopedics, Traumatology and Rehabilitation*, vol. 6, pp. 1–6, 01 2013.

[2] J. Grover, "Security of vehicular ad hoc networks using blockchain: A comprehensive review," *Vehicular Communications*, vol. 34, p. 100458, 2022, Elsevier Science Publisher.

[3] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014, wiley Publication.

[4] K.-A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012, IEEE.

[5] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient rsu-aided message authentication scheme in vehicular communication networks," in *in proceedings of International Conference on Communications*. Beijing, China: IEEE, 2008, pp. 1451–1457.

[6] C. Zhang, P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, pp. 1851–1865, 11 2011, Springer.

[7] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks." New York, NY, USA: Association for Computing Machinery, 2005.

[8] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *in proceedings of INFOCOM: The 27th Conference on Computer Communications*. Phoenix,AZ,USA: IEEE, 2008, pp. 246–250.

[9] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2792–2801, 2019.

[10] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *Transactions on Intelligent Transportation Systems*, vol. 22, no. 12, pp. 7408–7420, 2021, IEEE.

[11] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," in *proceedings of sInternational Conference on Consumer Electronics, Communications and Networks (CECNet)*. Xianning,China: IEEE, 2011, pp. 1758–1761.

[12] M. Wagner and B. McMillin, "Cyber-physical transactions: A method for securing VANETs with blockchains," in *proceedings of 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*. Taipei,Taiwan: IEEE, 2018, pp. 64–73.

[13] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, 2020.

[14] J. Wang, J. Huang, L. Kong, G. Chen, D. Zhou, and J. J. C. Rodrigues, "A privacy-preserving vehicular data sharing framework atop multi-sharding blockchain," in *Proceedings of (GLOBECOM): Global Communications Conference*, vol. 4. Madrid, Spain: IEEE, 2021, pp. 1–6.

[15] C. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*.

[16] J. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, 2004, IEEE. [Online]. Available: 10.1109/MSP.2004.26

[17] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," *in proceedings of the European Wireless Conference*, vol. 35, 01 2002, jjdewi.

[18] B. Aslam and C. Zou, "Distributed certificate and application architecture for VANETs," in *MILCOM 2009 - 2009 IEEE Military Communications Conference*, 2009, pp. 1–7.

[19] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, p. 39–68, jan 2007.

[20] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *2007 7th International Conference on ITS Telecommunications*. French Riviera, France: IEEE, 2007, pp. 1–6.

[21] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[22] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Transactions on Information Forensics and Security*, vol. 10, no. 12, 2015.

[23] F. M. Salem, M. H. Ibrahim, and I. I. Ibrahim, "Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks," in *2010 Sixth International Conference on Networking and Services*. Washington DC, USA: IEEE Computer Society, 2010, pp. 156–161.

[24] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for v2v communications," in *Vehicular Networking Conference*. IEEE, 2013, pp. 1–8.

[25] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *2007 Mobile Networking for Vehicular Environments*, 2007, pp. 103–108.

[26] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology — CRYPTO 2001*, J. Kilian, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 213–229.

[27] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117 716–117 726, 2019, IEEE.

[28] A. Patel, N. Shah, T. Limbasiya, and D. Das, "Vehiclechain: Blockchain-based vehicular data transmission scheme for smart city," in *proceedings of International Conference on Systems, Man and Cybernetics (SMC)*. IEEE, 2019, pp. 661–667.

[29] M. Li, J. Weng, A. Yang, J.-N. Liu, and X. Lin, "Toward blockchain-based fair and anonymous ad dissemination in vehicular networks," *Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11 248–11 259, 2019, IEEE.

[30] A. Mostafa, "VANET blockchain: A general framework for detecting malicious vehicles," *Journal of Communications*, pp. 356–362, 01 2019.

[31] N. Malik, P. Nanda, X. He, and R. Liu, "Trust and reputation in vehicular networks: A smart contract-based approach," in *2019 18th International Conference On Trust, Security And Privacy In Computing And Communications/13th International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2019.

[32] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *Internet of Things Journal*, vol. 7, no. 5, pp. 4101–4112, 2020, IEEE.