A Recent Survey on Authentication Schemes with Privacy Preservation in VANETs

*Raghupathi S
IBRI College of Technology, Oman
raghusenthil@gmail.com

Jaisankar N
VIT University, India
njaisankar@vit.ac.in

Anupriya E
IBRI College of Technology, Oman
dr.e.anupriya@ibrict.edu.om

Abstract: Vehicular Ad-Hoc Networks (VANETs) are one of the quintessential elements in imminent transportation systems. Vehicles in the VANET are interconnected with them and the infrastructures through a Dedicated Short Range Communication channel (DSRC) and utilize the IEEE 802.11p legacy as its communication protocol. Wireless communications are susceptible to a variety of attacks. Some of the assaults are false identification claim, monitoring victims and others. Hence, the communication among the automobiles and the infrastructures want to be blanketed towards attacks. VANETs furnish security services like authentication, anonymity, privacy protection, message integrity and others to mitigate the assaults on automobiles and the infrastructures in the network. Many research options which tackle these protection problems in the past. In this paper, some of the posted works of literature are reviewed which presents options to safety troubles like authentication and secluded safety and the solutions had been in contrast to get better understanding.

Keywords: VANET, Digital Signatures, Message Authentication, Privacy Preservation, Attacks, Cryptographic Systems.

I. INTRODUCTION

Past few decades witnesses the rapid advancements in the wireless communication technologies never before. Nowadays, transportation becomes intelligent and smart as Intelligent Transportation Systems (ITS). VANET is one of the many flavors of Mobile Ad-Hoc Network (MANET). VANET is a dedicated network meant for vehicles in the confine of the smart city. Smart Cities requires well-structured and efficient systems to regulate and provide smart services, safety to the commuters as well as operators and drivers for a hassle-free journey. Using present-day wireless technological advancements, transportation is connected among vehicles with inbuilt communication devices called On-Board Units (OBU). The communication among the network and the vehicles are termed in the name of messages and they are generally categorized as (a) Vehicle to Vehicle Communication (V-V), (b) Vehicle to Infrastructure Communication (V-I), (c) Safety Information and Non-Safety Information's and finally ,(e) Entertainment Information. VANET provides various application services among vehicles. According to the US Department of Transportation, the different types of VANET applications are safety and comfort, which are shown in Fig 1. VANET has these many components in its network namely (i) On-Board Unit (OBU), (ii) Road Side Unit (RSU) and (iii) Trusted Authority (TA).

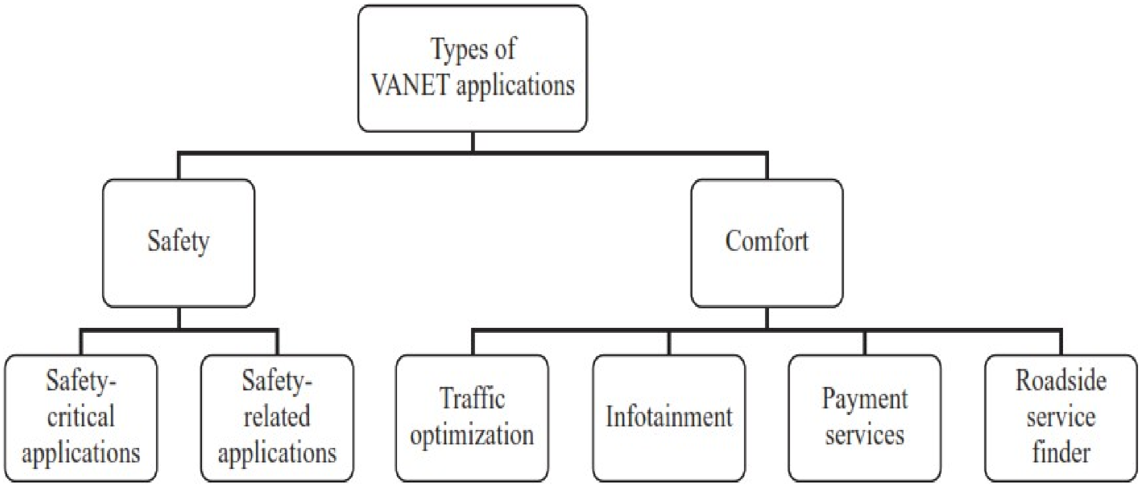

Fig. 1. Types of VANET Applications. (Adapted from [1])

Communication among vehicles will be in the form of small messages, and the authenticity of the messages should be verified by the receiver. Vehicles broadcast traffic-related and security related messages in the interval of 50-200 milliseconds. If the communication is not secured, then an adversary can intercept the messages, and they can extract information like the real identity of the vehicle or driver, vehicles location, position, and speed, etc. Using those intercepted and extracted information an adversary can do several kinds of attacks on the network and on an individual, some of the examples of attacks such as jamming, impersonating, privacy violation, forgery, in-transit traffic tampering, and onboard tampering. So, the network must provide robust security measures to connected vehicles. Some of the security measures in which the VANET provide are message authentication, message integrity, message availability, message non-repudiation, and Data confidentiality. Security services provided by VANET is illustrated in Fig 2.

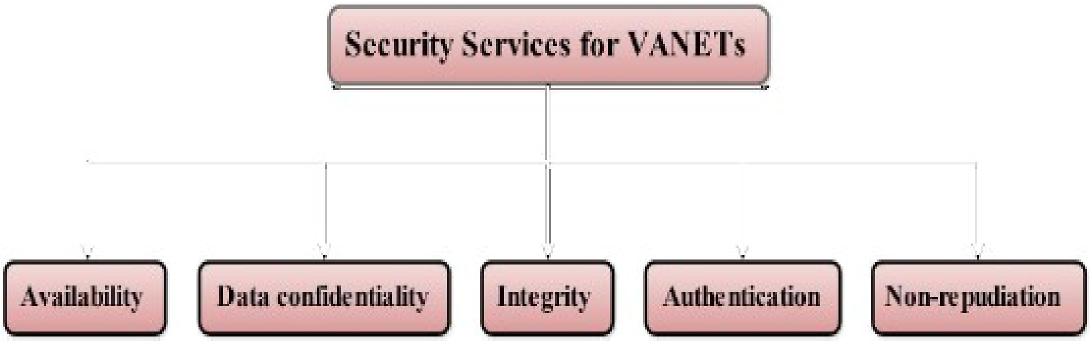

Fig. 2. Security Services. (Adapted from [2])

Message authentication is an important aspect and becomes crucial among vehicles in communication. This paper reviewed some of the previous works with providing solutions to authentication of messages using Digital Signatures and identity protecting privacy preservation schemes in VANET. The Organization of this review work is done and in the forthcoming section the previous works related to the privacy preservation and authentication were discussed whereas Section 3 discusses the various works for providing solutions to authentication problem and identity protecting privacy preservation schemes. Section 4 and 5 provides the overview of all the reviewed works in the form of a comparison table as well the concluding remarks.

II. PREVIOUS WORKS

Before the deployment of VANET in real-time use, it is necessary to satisfy all the security requirements, which mentioned previously in the introduction section. Many previous papers tried to provide solutions primarily based on some of the requirements. Raya and Hubaux [3] delivered a Public Key Infrastructure (PKI) based total scheme that previously loaded a mass of unknown certificates into vehicles, Tamper Proof Devices (TPD). The unknown certificates or the anonymous certificates include vehicles, lesser lifetime public/private keys. Hence the tracing could be avoided. Raya et al.'s scheme demanded that motors have sufficient storage space to shop public/private keys with their certificates, whilst the TA need to additionally shop all vehicles' certificates. Lu et al. [4] developed every other PKI-based scheme where RSU acted as semi-trusted authorities and generated brief nameless certificates for vehicles. This scheme avoids the large storage demanded, such as in Raya and Hubaux's scheme. However, cars have to often engage with RSUs to their unknown certificates. Thus, Lu et al.'s scheme is now not efficient. Lin et al. [5] gave an anonymous authentication scheme primarily based on ID-based signature (Shamir 1984) and crew signature (Boneh, Lynn, and Shacham 2004). In Lin's scheme, vehicles store the group public key and their personal keys. Wholly the messages that are signed through a vehicle without the vehicle's identity and apart it could be verified by any other receiver with a crew of public key. This scheme increases the tracing overhead as it requires the traced authority to keep up a Certificate Revocation List (CRL). Zhang et al. [6] adopted TPD to pre-load the machine master key for every vehicle, and then the TPD's generate the pseudo-IDs and its relevant signatures. At the equal time, the TA might need to hint the actual identification from vehicle's pseudo-ID. This scheme minimize the charge of verifying and transferring the public key certificates. Zhang et al.'s scheme [7] adopts batch verification of message signatures and can additionally decrease the ordinary verification delay. Similar to Zhang et al.'s scheme, there are many anonymous authentication schemes which preload the system master key into TPD (He et al. 2015 [8]; Tzeng et al. 2017 [9]). However, TPDs cannot resist side-channel attacks. Hence, an antagonist could extract the confidential records (Cilio, Linder, and Porter 2013 [10]; Ravi, Raghunathan, and Chakradhar 2004 [11]). Once a TPD is captured by a side-channel attacks, then the machine master key should be exposed, and the entire VANET would be a compromise. Shim [12] made an efficient ID-based anonymous authentication scheme, which was an extra secure due to the fact that the scheme utilize TPDS to pre-load the vehicle's personal key alternatively of the device master key. Liu et al. [13] found that Shim's scheme couldn't restrict the modification attacks. Zhang et al. [14] espoused one-time signature technology to figure out a distributed privacy- maintaining authentication rule, where RSUs will act as lower-level TA, generated secrets and techniques for vehicles. The secrets saved in TPD's could be well- run before the foes can capture TPDs. As, such this protocol is much less efficient due to the fact that too many communications concerning the vehicle's and the RSUs.

III. Classification of Authentication Schemes

In VANET, the authentication, security, and privacy are consumed to cultivate trust among V-V and V-I communications. Privacy is, everyone has the right to keep their information confidential and decide whether to share or not the same with other personnel. In specific, privacy is a system that is castoff to safeguard the profound and trusted material of the vehicles or commuters from the assaulter. Vehicle privacy must be taken care as an essential security concern in VANET. Thereafter, a quantum of research findings had done in the area of privacy and security in VANET, which warrants vehicle safety and enhances the traffic flow. Unknown authentication is a well- known approach. Pseudonym-based approach is reliable for the recent and existing workings, which can be used to protect the privacy and security of the vehicle users. By utilizing the pseudonym-based approaches, users can get better and more robust privacy preservation. To have more control over the privacy attacks, the TA should change the pseudonyms of vehicles frequently.

Privacy of Message in VANETs is still pigeonholed into two types namely,

(i) privacy of user protection and (ii) user location privacy.

Privacy of user Protection is used to prevent the malicious node not to access the personal information of user.

User location protection is to protect the user information, like route information and target location at prescribed time.

Authentication of messages sent between vehicles. The infrastructure is started after the vehicles are being registered with the Regional Transport Authority or Trusted Third Party Authority, where the vehicles public and partial private key is generated.

Most of the schemes use the Cryptographic techniques and signature techniques to endorse the verifying and the signing messages. Various Authentication schemes employed as of now in the research domain of VANETs is shown in Fig.3 and discussed below.

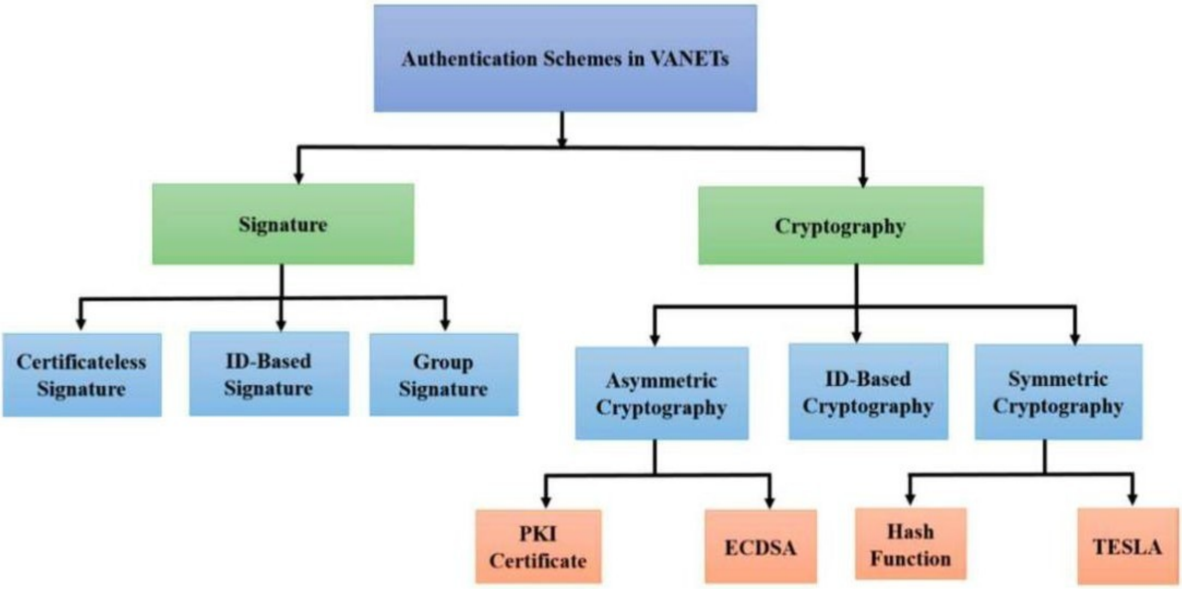

Fig. 3. Classification of Authentication Schemes in VANETs. (Adapted from [16])

Signature Scheme

Signature has the number of properties such as a person responsible for the document and it is verified easily by the third party. The further classification of the signature scheme is ID-Based signature; Certificate less signature and Group signature are briefed below.

Identity based signature schemes

Identity Based Signature (IBS) scheme routines nodule identifier in the order of the public keys and sign messages with the private key generated from the identifiers. In IBS, the Private Key Generator (PKG) is used as a TA for generating and assigning the private key. The Latest updation on a, new Identity-Based on sign Cryption (IBSC), a reliable as it introduces a bilinear pairing based on robust security forming by not allowing a random oracle background. Following terms such as setup, key extraction, signature signing and verification are the processing steps of IBS.

Setup: Public parameters are evaluated by PKG and then it releases those parameters to all vehicles visibly in the Network.

Key Extraction: same way PKG make use of vehicle ID and master ID to work out a private key and then the PKG transmit those private keys to communicate with the vehicle through a reliable channel.

Signing Signature: SIG could be generated by making a private key on an assumption of a message (m), and a timestamp (t).

Verification: Verification algorithm is utilized to check the signatures SIG is validity by having some parameters like identity, signature, and message.

Certificate less Signature Schemes

The trouble which is faced in IBS could be resolved by Certificate Less Signature (CLS) scheme which chokes the high cost certificates based on method of PKI. In the year 2003, the certificates less public key mechanism was once presented for the very first time. In CLS, the Key Generation Centre (KGC) plays a vital role, which functions as a third party and take responsibility to offer the private key to the user, which is weighed through the consumer ID. The stealthy values that a consumer can breed contains the private key and the half personal keys are supplied using KGC. Similar to the ID based cryptographic scheme, the KGC might not have right of entry with this type of private key. Due to that, a user could make use of secret values and exclusive factors to yield the public key access. The CLS technique is categorized into seven one-of-a-kind algorithms, such as sign, verify, setup, set secret value, Partial private key extract, set personal key and set public key.

Group Signature Schemes

Signature based schemes preserves the vehicle privacy which would allow only the registered members of the group to act for the anonymous messages as a group representative. The group head gains the right to detect the incoming sign from the original source. This scheme meant a major quantum of time to endorse the signature, which sorts it restrictions to the applications related to time in VANETs.

Cryptography Schemes

Cryptography is used to prevent private information from the public and also from the third parties. The cryptography schemes are further classified into Asymmetric, ID-Based and Symmetric Cryptography. A brief note is discussed below.

Asymmetric Cryptography Scheme

Asymmetric cryptography is also known as public-key cryptography. This method can be used for encrypting and decrypting a message to ensure the protection of data in the major verbal exchange network. Specifically, the asymmetry can be used to encrypt a message, which can be performed both by means of using a public key and by using producing a digital signature. Usually, a personal key is only used for decrypting an encrypted message and for verifying the digitally-signed message. Asymmetric cryptography is in addition labeled as a PKI certificates and Elliptic Curve Digital Signature based Authentication (ECDSA) schemes.

Public Key Infrastructure Certificate Schemes

Most of the cars incorporate public or private key for pseudonymous communication. In order to obtain a invulnerable and reliable way, the public key certificates are the excellent techniques that are used in PKI to authenticate vehicles.

Elliptic Curve Digital Signature Based Authentication Schemes

The other phase of asymmetric cryptography is an ECDSA authentication scheme, which is an analog kind of digital signature established on the elliptical curve cryptography. Manvi et al. supplemented an ECDSA-based message authentication scheme in VANET. This approach utilizes a Secure Hash Algorithm (SHA) by the sending car to generate a personal and public key and also create a hash of the message by way to use SHA. At the destination part, the obtained message is decrypted by using the public key.

Identity Based Cryptography Schemes

Identity Based Cryptography is like an asymmetric cryptography, where the user public key could be derived through their ID records as such person location, telephone number, email ID. In a way to authenticate the message, the IBC authentication schemes did not use the PKI certificates. Hence resulted the drastic reduced the communication overhead as well it manages the overhead of CRLs.

Symmetric Cryptography

Symmetric-key cryptography makes use of the same cryptographic keys for each encryption and decryption of messages. The keys may additionally be identical, or there might also be a easy transformation to go between the two keys.

Hash Function Based Authentication Schemes

Yet another category of symmetric cryptography is the Hash Function. Its responsibility is to audit the message integrity when it encounters a data encryption. As well it generates the fixed string which refers the equivalence of hash value. This is essential that the hash value is required to connect with the messages by the same way to reach the target, the message Integrity.

TESLA-Based Authentication Schemes

The extension of symmetric cryptography is the Time Efficient stream Loss Tolerant Authentication (TESLA).In this scheme the source calculates Message Authentication Code (MAC) the use of a known key and appends the authentication code to every transferring message, as well the reception information's are buffered except authentication at the detection end. The most important demerit of TESLA is that it develops a clock synchronization pulse in the receiving end as it is enough to have it in the transmitting end. Apart TESLA is susceptible to DOS attacks in phrase of memory occupation which is introduced by the use of unregistered vehicles. Thus, the intention of the scheme is to pick out malicious points and spurious messages, and hence, it can capable to supply safety in VANETs.

The grouping of authentication schemes in each category is mentioned by the nature of evaluation and their associated workings as follows.

Majid Bayat et al. [17] proposed a new and novel scheme for authentication for VANETs, without any need to have crew signatures, the involvement of RSU, Pseudo identities, and TPD. This paper employs the ECDSA approach to generate digital signatures, signature verification, and to trace the malicious vehicles which claim false identity. The scheme consists of four phases' initialization, registration, message authentication, and verification and the effectivity of the scheme is determined to be 300ms to confirm the signature.

Avleen Kaur Malhi et al. [18] introduced the CLS scheme for VANETs, which combines all the signatures and verifies them in a combination manner, therefore reducing the signature verification time considerably. It used to be assumed that all the vehicles possess an ID at the purchase which is allotted to them solely after registering the non-public details of the car owner. Thereafter, these ID's are stocked in the database of the TA. As a prime behavior of VANET is its scalability, it proves it an environment friendly CLS scheme which is proposed for inter-vehicle communication. This scheme is efficient in contrast to the others by it verifies the node and its signature with a figure of 124.6ms for a cycle of 50 nodes.

Hui Liu et al. [19] proposed a new model of the VANETs communication system, which can be realized by way of the lattice-based signature scheme. Based on the lattice-based signature scheme, a secure, nameless authentication scheme is constructed which affords privacy-preserving V2I and V2V communications besides TPDs. The proposed nameless authentication scheme contains 4 phases: device initialization, personal key extraction, signature generation, and message verification. The out rate performance evaluation show that the proposed scheme is more environment friendly than previous solutions. The protection analysis demonstrates that this scheme is secure against forgery attack. The lattice dimension used is 251, in accordance to NTRU standards. The time to compute the signature and verification for 105 trials is 1.409µs, 1.18µs.

Hong Zhong et al. [20] Proposal of new idea to sign the messages exchanged between V-I and V-V primarily based on Bilinear mapping cryptographic scheme. This additionally affords combination message verification scheme, which reduces the computational and communicational overhead that incurs if the OBUs, RSUs has to affirm significant messages. The proposed scheme is utilized bilinear maps, and the security of the proposed scheme is primarily based on Computational Diffie-Hellman (CDH) problem. Divide the sign section into two steps and utilize the pre-calculation technique to decrease the computation cost in signal phase. RSU of signatures into a single one, and the size of aggregated signature can mix a couple of steady measurement which notably reduces the transmission overhead between RSU and application server and the effectivity of verification for software is improved. The time to compute the Hash and the signature is TH, Ts is 0.09ms, 0.39ms.

M.Rekik et al. [21] proposed an enhancement to before work [22] which gives an answer for authentication problem as, dual authentication with key management. The enhancement achieved in this work is introducing extra authentication segment and a re-authentication phase, with the aid of retaining the amount of data required to compute for the authentication in a computationally environment friendly way. This used to be tested the use of the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Performance validation used to be additionally done with Open SSL device to prove that lengthen in the course of the computation of authentication information is promising with such robust security. The proposed options lengthen for computing dual authentication is 0.03ms when in contrast to the previous solution's 5.3ms.

The evaluation of preceding works that provides a security solutions in VANETs on the basis of the techniques, efficiency, and optimizations are shown under in Table.1.

Table. 1. Comparison of Various Previous Works Providing Security Solutions in VANETs.

Sl No.	Author	Security Mechanisms Implemented		Crypto Algorithms Used	TPD Used	Pseudo Identity Used	Certificate Used	Efficiency Of the Proposed Scheme	Optimization
		Authentication	Privacy Protection						
01.	Avleen et al.	Yes	Yes	Bi-linear Maps	No	No	No	3(T_{pair}+T_{mul}) is 124.6 ms for 50 nodes	Not Done
02.	Hui Liu et al.	Yes	Yes	Lattice-Based Signature Scheme	No	No	No	10^5 Trials in 1.409µs, 1.18µs	Not Done
03.	Majid Bayat et al.	Yes	Yes	Elliptic Curve Based Signature	No	Yes	No	3T_{pair}+ T_p is 0.027287 s	Not Done
04.	Hong Zhong et al.	Yes	Yes	Bi-linear Maps	No	Yes	No	T_H, T_S is 0.09ms,0.39ms	Not Done
05.	M.Rekik et al.	Yes	Yes	Generic PKI	No	Yes	No	T_S is 0.03162ms	Optimization Done

Notations: TPD : Tamper Proof Device
T_{pair} : Time to Pair
T_{p} : Time to Process the computation of Paired devices signatures
T_{H} : Time to compute the Hash Value
T_{S} : Time to Generate the Digital Signature

IV. CONCLUSION

VANET is the most researched topic in current and past decade of computer network research community. Due to the high feasible near future implementation, it draws the attention of all pc network scientists. In this paper, some of the vital safety solutions in the VANETs that is authentication, with privacy protection had been furnished from the quantum related literature work. When an excessive range of nodes or vehicles involved in VANETs, the computational overhead due to verify and authenticate nodes on the fly will become crucial. Hence a robust, resilient and computationally efficient authentication scheme is needed. Based on the learning, the effect of the review states that, it is a requisite to design an authentication scheme which can outperform the method for volumes of data.

References

[1] A.K. Malhi, S. Batra, & H.S.Pannu, (2019).“An Efficient Privacy Preserving Authentication Scheme for Vehicular Communications”, Wireless Personal Communications, Vol.106, Issue.2, pp.487–503.

[2] C. Zhang ,R. Lu , X. Lin , P.-H. Ho , X. Shen, (2008).“An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks”. 2008 Proceedings IEEE INFOCOM - The 27th Conference on Computer Communications.

[3] Debiao He, Sherali Zeadally, Baowen Xu, Xinyi Huang, (2015). “An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks”, IEEE Transactions on Information Forensics and Security, Vol.10, Issue.12, pp.2681–2691.

[4] HongZhong, ShunshunHan, JieCui,, JingZhang, YanXu , (2019). “Privacy-preserving authentication scheme with full aggregation in VANET”, Information Sciences, Vol.47, Issue.6 pp.211–221.

[5] H. Liu, Yining Sun , Yan Xu, Zhuo Wei, (2019).“A secure lattice-based anonymous authentication scheme for VANETs”, Journal of the Chinese Institute of Engineers, Vol.42, Issue.1, pp.66–73.

[6] Joseph K.Liu,Tsz HonYuen , Man HoAu ,WillySusilo, (2013). “Mitigating power- and timing-based side-channel attacks using dual-spacer dual-rail delay-insensitive asynchronous logic”, Microelectronics Journal, Vol.44, Issue.3, pp..258–269.

[7] Joseph K.Liu,Tsz HonYuen , Man HoAu ,WillySusilo, (2014). “Improvements on an authentication scheme for vehicular sensor networks”, Expert Systems with Applications, Vol.41, Issue.5, pp.2559–2564.

[8] K.A. Shim, (2012).“Cpas: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks”, IEEE Transactions on Vehicular Technology, Vol.61, Issue.4, pp..1874–1883.

[9] L. Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Chuanyan Hu , (2017). “Distributed Aggregate Privacy-Preserving Authentication in VANETs”, IEEE Transactions on Intelligent Transportation Systems, Vol.18, Issue.3, pp.516–526.

[10] Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Chuanyan Hu, (2017). “Distributed Aggregate Privacy-Preserving Authentication in VANETs”, IEEE Transactions on Intelligent Transportation Systems, Vol.18, Issue.3, pp.516–526.

[11] M. Azees, L. Jegatha Deborah & P. Vijayakumar, (2016).“Comprehensive survey on security services in vehicular ad-hoc networks”, IET Intelligent Transport Systems, Vol.10, Issue.6, pp.379–388.

[12] M. Bayat, Barmshoory, Mostafa, Rahimi, Majid, Farjami, Yaghoub, Mohammad Reza Aref , (2019), “A new and efficient authentication scheme for vehicular ad hoc networks”, Journal of Intelligent Transportation Systems, pp.1–13.

[13] M. Raya, and J.P. Hubaux, (2007). “Securing vehicular ad hoc networks”, Journal of Computer Security, Vol.15, Issue.1, pp.39–68.

[14] M. Rekik, Amel Meddeb-Makhlouf , Faouzi Zarai , Mohammad S. Obaidat , (2017). “Improved Dual Authentication and Key Management Techniques in Vehicular Ad Hoc Networks:, 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA).

[15] M.S. Sheikh, & J. Liang, (2019). “A Comprehensive Survey on VANET Security Services in Traffic Management System”, Wireless Communications and Mobile Computing, pp.1–23.

[16] P. Vijayakumar, Maria Azees, Arputharaj Kannan, Lazarus Jegatha Deborah, (2016). “Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks”, IEEE Transactions on Intelligent Transportation Systems, Vol.17, Issue.4 pp.1015–1028.

[17] R. Lu, et al, (2008). “Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications”, In the Proceedings of 2008 IEEE INFOCOM - The 27th Conference on Computer Communications.

[18] Shiang-Feng Tzeng , Shi-Jinn Horng , Tianrui Li , Xian Wang , Po-Hsian Huang , Muhammad Khurram Khan, (2017).“Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs”, IEEE Transactions on Vehicular Technology, Vol.66, Issue.4, pp.3235–3248.

[19] Sheikh, Liang & Wang, (2019). “A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)”, Sensors, Vol.19, Issue.16, p.3589.

[20] S. Ravi, A. Raghunathan, & S. Chakradhar, (2004). “Tamper resistance mechanisms for secure embedded systems”, 17th International Conference on VLSI Design.

[21] Tellez and Zeadally, (2013). “Security in vehicular ad hoc networks”, pp.49–78.

[22] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, Xuemin Shen, (2007). “GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications”, IEEE Transactions on Vehicular Technology, Vol.56, Issue.6, pp.3442–3456.