2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering

Blockchain Based Secured Identity Authentication and Expeditious Revocation Framework for Vehicular Networks

Nisha Malik[1], Priyadarsi Nanda[1], Arushi Arora[2], Xiangjian He[1] and Deepak Puthal[1]
[1]Faculty of Engineering and IT, University of Technology Sydney, Australia
[2]Computer Science Department, Indira Gandhi Delhi Technical University for Women (IGDTUW), New Delhi, India.
Email: <Nisha.Malik,Priyadarsi.Nanda,Xiangjian.He,Deepak.Puthal>@<uts.edu.au>[1], arushi1250@gmail.com[2]

Abstract— **Authentication and revocation of users in Vehicular Adhoc Networks (VANETS) are two vital security aspects. It is extremely important to perform these actions promptly and efficiently. The past works addressing these issues lack in mitigating the reliance on the centralized trusted authority and therefore do not provide distributed and decentralized security. This paper proposes a blockchain based authentication and revocation framework for vehicular networks, which not only reduces the computation and communication overhead by mitigating dependency on a trusted authority for identity verification, but also speedily updates the status of revocated vehicles in the shared blockchain ledger. In the proposed framework, vehicles obtain their Pseudo IDs from the Certificate Authority (CA), which are stored along with their certificate in the immutable authentication blockchain and the pointer corresponding to the entry in blockchain, enables the Road Side Units (RSUs) to verify the identity of a vehicle on road. The efficiency and performance of the framework has been validated using the Omnet++ simulation environment.**

Keywords—Blockchain, Authentication, Revocation, Security, Vehicular Networks

I. INTRODUCTION

Privacy and security in Vehicular Ad Hoc Networks (VANETs) have gained huge prominence after Vehicle Safety Communication (VSC) project [1], delivering the concept of pseudonym certificates for vehicles and effectively safeguarding the communication within the network for a comfortable and safe driving experience. The self-structured technology entails Vehicle to roadside Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) wireless communication using Dedicated Short-Range Communication (DSRC) of 5.9 GHz band, with a bandwidth of 75 MHz and an approximate range of 1000m [2]. The cloud servers deployed in the conventional centralized mechanism in VANETs serve as an excellent bait for the attackers as a single point of failure leading to certain treacherous situations and disrupting the entire network. In addition, the malicious messages from suspicious parties or alteration in genuine messages influence the driver's behaviour and can cause mishaps jeopardizing the safety of passengers on road. Lack of privacy and security breaches, for instance, tracking of a vehicle, impose a restriction on using them for providing personalized services.

The next-generation immutable blockchain technology made its appearance in 2008 along with the cryptocurrency-Bitcoin [3], effectively securing and decentralizing the way data is managed and stored, thereby, reducing the role of the middleman or a third party. The cryptographically sealed and consensus-based blockchain architecture uses the concept of a synchronized distributed public ledger, a copy of which abides in all the nodes and the blocks of the ledger are encrypted and chained together in a chronological order. A pair of a public and private key is associated with each node of the network. A block, which is the basic building unit of the chain, encompasses the transactions, its hash value, timestamp, a signature of the block and nonce. A transaction is signed with a private key of the sender and public key of the receiver. Miners are special nodes of the network, which compute a complex puzzle [3] to include the block into the chain within a specified time and are incentivized for the same.

Though most of the researches in VANETS focusing majorly on the security aspect have predominantly addressed authentication and conditional privacy issues, but they lack to suffice the scalability, efficient authentication, quick check on revocation and reducing dependency on the centralized authority. In proposed work, users associate with the *CA* only in the registration step, post which, on-road authentication, verification, and revocation of vehicles is performed by the *RSUs* using the shared blockchain ledger. Security requirements with user anonymity are fulfilled by the shared ledger, which reduces the steps in authentication and performing secure communication.

The paper is organized as follows: Section II presents the related work, Section III elucidates research motivation. In section IV, the proposed framework is given. Section V details the implementation and results followed by section VI and VII, which focus on theoretical analysis and conclusion respectively.

II. RELATED WORKS

The open access environment catered by VANETs instigates open challenges in the field of privacy and security making it unfit for implementation in the real world [4-8]. In a study, pre-shared keys were introduced to implement the authentication of nodes in the network [9]. Calandriello et al. [10] focused on security and

2324-9013/18/31.00 ©2018 IEEE
DOI 10.1109/TrustCom/BigDataSE.2018.00099

privacy in VANETs and proposed a hybrid method, which strengthens the framework using pseudonyms with self-certification, thus, eliminating the need for managing them without compromising on the robustness of the system. To obtain high accuracy and privacy with respect to the vehicle's location, Memon et al. [11] developed a methodology based on dynamic pseudonym generation for mix-zones environment and verified the results using the SUMO simulator.

With the launch of Bitcoin blockchain [12] in 2008, the focus of industry and academia shifted towards approaches which could secure the way centralized networks operated [13]. From then on, some researches in VANETs focused on methodologies to improve efficiency, guaranteeing privacy and security using the blockchain technology. Yuan et al. [14] introduced a seven-layer secure and decentralized conceptual model for Intelligent Transport System (ITS), discussing the relationship between Blockchain-based ITS and parallel transportation management systems claiming the former to be the future of ITS. After the introduction of autonomous/self-driving vehicles on the road for which efficient and timely communication amongst the nodes is of utmost importance, Rowan et al. [15] explored the use of sensing and signalling devices using blockchain public key infrastructure and an inter-vehicle session key establishment protocol. The decentralized framework proposed in this paper is claimed to be secure and trustable, thus providing reduced *CA* dependency, authentication with minimal overheads and communication with validation check.

III. Research Motivation

When vehicles begin their travel on road, the infrastructure should uphold the monumental purpose of user safety and security for administering and provisioning these services. Authentication and authorisation of network users with reduced latency is the most essential part, considering the dynamic nature of the network. Keeping all these scenarios into consideration, we have derived our problem statement, which is broadly categorized into the following requirements.

Mutual Authentication with Reduced Dependency on CA: Mutual authentication between OBU and RSU should not involve complex computations or frequent communications with the CA unlike some earlier schemes [17].

Scalability: The framework should reckon with scalable attributes to the vastness of vehicular networks.

Privacy Protection: The authentication of users should not incur at the cost of their identity disclosure or perturbing their privacy.

Message Confidentiality, Integrity and Non-Repudiation: The security mechanism should verify authenticity and integrity and prevent unauthorized access by intruders, to avoid any compromise of confidentiality and authentication to prevent repudiation.

Speedy Revocation Without Additional Overhead: The framework should not just be able to perform authentication, but quickly revocate the malicious vehicles. The vehicles revocated should be easy to identify without circulating an entire Certificate Revocation List (CRL) as it causes lot of overhead.

The novel blockchain-based framework proposed in this paper ensures privacy and security of vehicles in the decentralized network. Here, a private blockchain is used which gives selective access to ledger, where Revocation Authority (*RA*) and *CA* have complete control over the ledger, giving *RSUs* only read rights, and no rights to *OBUs*, hence avoiding any exposure to untrusted entities. The hash table and pointer to the ledger entry, which reside with the *CA* support traceability of vehicles, in case of any suspicious behaviour. This framework makes use of no POW (Proof-of-Work) [3] mechanism, hence, reducing the computational costs. We have used the Proof-of-authority [16], whereby access rights are issued based on predefined authority. The framework eliminates the need of any CRL and makes it easy with a quick step to discover a node's revocation.

IV. Proposed Framework

This section presents functioning of the proposed framework, which is unique due to the introduction of a private blockchain in authentication and revocation. This blockchain mainly contributes in the operation of the framework by reducing dependency on the *CA*.

A. Fundamental Operation of the Framework

The notations used in the proposed framework are given in Table 1. The physical entities, i.e. *CA*, *RA*, and *RSU* collaboratively communicate via the shared ledger to achieve the security for *'safety-on-road'* motive which is explained in the following three phases briefly.

TABLE I. Notations

Notation	Meaning
→	Unicast communication
--))	Broadcast Communication
#	An entity stores the data in the data structure following it.
*	An entity operates on the data structure/object following it.
H ()	Hash function
{} DS_X	Digitally signed by X
E_X ()	Encrypt with X
D_X ()	Decrypt with X
Verify ()	Function to check integrity and authenticity of a message.
M_i	Message
Group ()	Function to include a vehicle in the group after authentication
Query ()	Function to search Pseudo ID of the OBU in β
B	Authentication and revocation ledger
Ptr_i	Pointer to the ledger entry
$HPrev_j$	Previous hash of the block
S_{RSUi}	Private key of i^{th} RSU
Tx_i	i^{th} transaction of block X in the ledger
TID_{Bi}	Transaction ID of i^{th} transaction of block B, given as H(input transaction)
MAP ()	Mapping function
V_i	i^{th} vehicle

B. System Initialization

The framework focuses on reducing dependency on the *CA* but does not completely deny its importance in the dynamic vehicular networks. During system initialization, different participants prepare to be occupied with numerous domain parameters required for later security operations. The *CA* builds the system for the ECC based PKI, by establishing the system parameters $X=p$, a, b, G, n and h for the curve C_p in the field F_p. Here, integer p defines the field F_p, a and b are constants defining the curve equation, G is the generator of the cyclic group Z_p, n which determines the order of G, is a prime number and h is the curve's cofactor given by $h= (1/n) |C(Fp)$. These parameters along with the publicly known hashing functions are stored in the vehicles during registration. In addition, the RSUs are supplied with the *CA*'s public key for signature verification in the ledger. *CA* generates its public key with its private key given by $P_{CA}= x. G$, where x is the private key of *CA*.

The blockchain network among the *CA*, *RA* and *RSUs* is setup by their public keys, through which they address and verify each other while storing and retrieving transactions. The genesis block for the authentication and revocation ledger is securely generated. Here, the *CA* creates new Identities, just as new coins are generated in the bitcoin blockchain. Apart from these, vehicles are assumed to obtain their Vehicles' ID before registration from the Motor Vehicle's Division (*MVD*).

C. Registration of the Vehicle

The users register with the *CA* for the first time by submitting their *VID* obtained from the *MVD*. The *CA* verifies the VID_i, assigns a Pseudo ID (PID_i) and generates an ECC Public-Private key pair namely P_{ki} and S_{ki}. The mapping of the actual identity with the assigned PID_i is stored in a hash map in its database. This ensures easy lookup in case of traceability and revocation of malicious users. The PID_i issued is digitally signed by the *CA* and forms a transaction of the Block β in the ledger.

TABLE II. REGISTRATION OF THE VEHICLE V_i WITH CA

1. $V_i \rightarrow CA$: ⟨VID_i, Other Details⟩
2. $CA*VID_i$: ⟨Verify (VID_i)⟩
3. $CA \# T_{Bi}$: ⟨input→ (PID_i)DS_{CA}⟩
⟨output 1→ (OP_Return "H($Cert_{PIDi}$"))⟩
⟨output 2→ Script: Verify (H(PK_{RA}), Sig_{RA}))
Value: val_0⟩
4. $CA \# \beta$: Update Ledger with the transaction
5. $CA \rightarrow V_i$: ⟨PID_i, Certificate (PID_i, DS_{CA}), ECC (P_{ki}, S_{ki}),
TID_{Bi} $Hash\_pointer_B$, H_Prev_B⟩
6. $CA \#$ ***Hashmap***: ⟨MAP (PID_i||VID_i)⟩

The input of the transaction can be easily verified as it includes *CA*'s public key hash address and its ECDSA signature. The output of the transaction is the most important part for identity verification. There are two outputs corresponding to each input for a new vehicle registration. The first output is the hash value of the certificate $Cert_i$ embedded in the OP_Return instruction of the output script. For an output script without an OP_return, the output is redeemed with the public-key-hash of the recipient and a signature verification called as '*Pay-to-pubkeyhash*' [3]. The transaction redeeming this output needs to provide an appropriate hash value, generated using its public key and signed using the corresponding private key. Thus, for redemption, the output script should evaluate to true with the above conditions satisfied and the output being an unused transaction output (UTXO). However, an output script containing the OP_return has no amount to be redeemed and thus the output script evaluates to be false. This output is only used to verify the authenticity of the certificate by matching it with the one sent by the *OBU*. The second output assigns a small amount of 0.02$ to the *RA*, which is redeemed by the *RA* in case of the vehicle going rogue and thus setting up the 'revocation flag' in the revocation transaction, thus, redeeming this amount. Post creation of the transaction, SHA-256 hashing function is used to compute the block's cryptographic hash as $HOB_{\beta i}$ = H (T_{Bi}, $HPrev_j$) and the ledger is updated. The result forms the hash previous for the next block, which is uploaded to Ledger β shared among the *CA, RA* and *RSUs*.

Conforming to the bitcoin transactions, these are also added by the *CA* in the chronological order and there is no serial number. Each transaction has a transaction Id (*TID*) that unlike the bitcoin transactions is just the hash of the input transaction, digitally signed by the *CA*. This ensures its verification. The steps of registration are depicted in Table 2.

However, since this is a private blockchain with no proof of work, with a layer of access control on the top of the shared ledger and a few positive assumptions, transactions can be modified in an extreme case. The *CA* then returns $Hash\_pointer_B$, assigned PID_i with corresponding certificate, and TID_{Bi} to the OBU. The ECC key-pair (P_k and S_k) are stored in the *OBU's* TPM.

D. Mutual Identity Authentication and Revocation

When the *OBU* is active on the road, it authenticates itself with the *RSU* and becomes part of the group of vehicles in range of the *RSU* as shown in Fig 1. The identity R_i of the *RSU*, obtained from the *CA,* serves both as its Identity as well its Public key. When the *OBU* comes in the range of the first RSU on road, it is notified from the *OBU*, since it contains all requisite identity information and certificates of the nearest RSUs stored in it. The *OBU* forms a message M containing its $Hash\_pointer_B$, TID_{Bi} and Ptr_i, *which* is encrypted with *Ri* using IBE scheme as shown in table 3.

The RSU upon receiving the message decrypts it with its private key S_{RSU}, and gets the PID_i, corresponding ledger entry and pointer to the block. It queries the blockchain using the PID_i as the index and when found, verifies both the outputs for the respective transaction. Once confirmed, the *RSU* sends a challenge integer (say *'n'*) to the *OBU* encrypted with its public key and waits for the response. If the *OBU* could decrypt the challenge message and send response as the next positive integer (*'n+1'*), it is authenticated by the RSU. The OBU is provided with the corresponding group key. Now, post

authentication, the new vehicle becomes part of the group of vehicles in the range of the RSU and is hence authorized to request any data, send information accumulated from the surroundings or receive emergency alerts from the RSU.

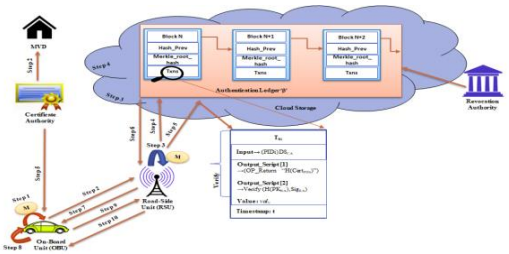

Figure 1. Mutual Authentication of OBU-RSU

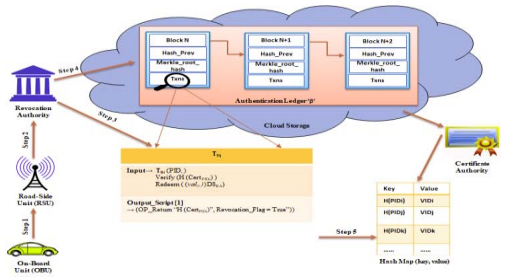

Figure 2. Revocation of malicious vehicle

TABLE III. MUTUAL IDENTITY AUTHENTICATION: OBUS FIRST ENCOUNTER WITH A RSU OR CHANGING RSU

1. *OBU$_i$*M$_i$:	⟨*PID$_i$*, Cert$_{PIDi}$, *E$_{Ri}$* (Hash_Pointer$_B$ || *TID$_{Bi}$*) ⟩
2. *OBU$_i$* → *RSU$_i$*:	⟨*M$_i$*⟩
3. *RSU$_i$M$_i$:**	⟨D $_{SRSUi}$ (Hash_Pointer$_B$ || *TID$_{Bi}$*) ⟩
4. *RSU$_i$β:**	⟨Query(β||*PID$_i$*) ⟩
5. *RSUT$_{Xi}$:**	Verify(H(Cert$_i$) *stored* = H(Cert$_i$) *received*)) *val$_0$* → not redeemed and Revocation Flag = False, if true go to step 6, else, do not authenticate.
6. *RSU Cert$_i$:**	⟨Extract *P$_{ki}$*⟩
7. *RSU$_i$* → *OBU$_i$*:	⟨E$_{Pki}$ (Challenge integer N) ⟩
8. *OBU(Challenge):**	⟨D$_{Pki}$ (Challenge integer N) ⟩
9. *OBU$_i$* → *RSU$_i$*:	⟨E$_{Pki}$ (Challenge-Response Integer N+1) ⟩
10. *RSU$_i$* → *OBU$_i$*:	⟨Group(*OBU$_i$*)⟩

For revocation, suppose the *RSU* receives a message from a malicious node and the message content is proven fallacious, then in such a scenario, the *RSU* would communicate with the *RA* sending the 'bogus message' as well as the *PID$_i$* responsible (Table 4). This transaction corresponding to the *PID$_i$* is verified by the *RA* and for initiating revocation of this *PID$_i$*, *RA* creates a new 'revocation transaction' taking the current *PID$_i$ registration* transaction as the input transaction and redeeming the 0.02$ in its output, thus setting the *revocation flag = true*. The original transaction is only verified without updating, and a new revocation transaction is generated, so that, when the malicious vehicle tries communication with the RSU, it can be identified through the revocation flag. In addition, the immutable nature of the ledger is not tampered. Also, the Hash map is updated accordingly by the *CA*. Now, *RSUs* instead of looking for a CRL can now easily verify the status by a transaction as shown in Fig 2.

TABLE IV. REVOCATION OF MALICIOUS VEHICLE

1. *V$_i$* → *RSU$_i$*:	(" Bogus Message" ⟩
2. *RSU*→*RA*:	⟨E$_{PKRA}$ (*PID$_i$*||'Bogus Message') ⟩
3. *RA* # *T$_{Dj}$*:	⟨input→ (*PID$_i$* || H (Cert$_{PIDi}$) || (*val$_{0j}$*) DS$_{RA}$⟩ ⟨output 1→ (OP_Return "H (Cert$_{PIDi}$)", Revocation Flag = True")) ⟩
4. *RA* # *β*:	⟨Update Ledger with the Revocation transaction⟩
5. *CA #HashMap*:	⟨ Search Revoked *PID* and delete entry⟩

For an emergency scenario detection, we assume *RSUs* to form a Mesh Network and hence easy connectivity and reachability is attained. Upon detection of an event, the *OBU* forms a message, which is verified by the *RSU* and forwarded either to the group of vehicles in range or to *RSU* of the respective area using an appropriate routing protocol. This avoids network flooding with the broadcast messages. Also, as the vehicles are authenticated by the RSU and are part of a group, RSU maintains a group table after authentication, to elude repeated ledger check for these vehicles.

V. IMPLEMENTATION AND RESULTS

A. System Setup

To demonstrate functionality of the proposed protocol, we have used the Veins [18] framework, which supports a range of models to display both the road traffic and network simulation. For network simulation we have used OMNeT++ 4.6 (Objective Modular Network Testbed in C++), which is a discrete event simulator.

TABLE V. SIMULATION PARAMETERS

Simulation Parameter	Value
Simulation time	6000s
Frequency	5.9 GHz
Number of nodes	1-100
Size of ground	5000m
Packet size	100-200 bytes
PHY Layer	IEEE 802.11P
MAC Layer	IEEE 1609.4
Data Rate	18Mbps
Measured parameters	Delay, Throughput and packet delivery ration (PDR)

To prototype intermodal traffic systems, SUMO-0.19.0 (Simulation of Urban Mobility) framework is used as the mobility generator to test and optimize the potent and efficiency of the proposed framework. The simulation is run on a Windows 7 (ultimate -x86) operating system with 8 GB of RAM. The simulation parameters are listed in Table 5.

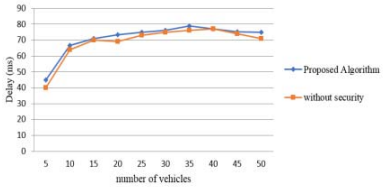

Figure 3. End-to-end delay performance

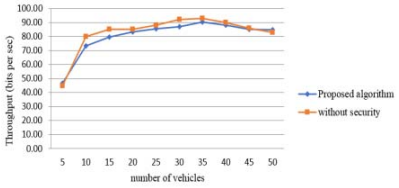

Figure 4. Throughput with increasing vehicles

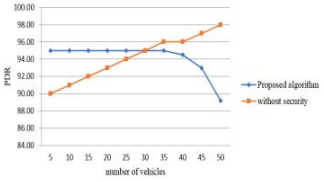

Figure 5. PDR with increasing v

The vehicles in the sumo simulator are shown as the dynamic nodes in the Omnet framework, where we code their functionality and behavior while in movement utilizing the inbuilt libraries and procedures. For our testing, the number of vehicles range from 1- 50, with speeds ranging from 14 to 20 m/s. The parameters associated with delay, throughput and PDR have been considered to showcase how the protocol performs, and the average values over an interval of every 5 vehicles is gathered.

The scenario consists of two *RSUs* located on road and authenticating vehicles by means of the shared ledger. The above-discussed parameters are evaluated for assessing the performance as they could successfully depict how addition of a few fields in the message communication, and encryption and decryption of messages affected the original working. Detailed analysis of the results under these parameters and the mentioned simulation setup are examined in the following subsection.

B. *Performance Analysis*

The protocol performs comparatively well considering the time taken with and without addition of security features. The difference in performance occurs due to the time consumption in executing the security operations, thus establishing the security requirements. The proposed protocol has been analyzed based on three parameters i.e. delay, throughput, and packet delivery ratio (PDR) with unicast communications between the vehicles and *RSUs*. The graphs show the comparison of the framework before and after applying the security features of encryption, decryption, verification and authorization for successful authentication and access control. The delay at *RSUs* increases with the increasing number of vehicles due to the time taken by encryption, decryption and ledger verification for upholding identity and confirming revocation simultaneously.

C. *End-to-End Delay and Throughput*

End-to-end delay between the *OBUs* and *RSUs* is the most important factor in assessing the performance as it evidently depicts how an additional overhead of encryption and decryption increases the delay in processing and response from the receiving RSU. We have only considered the computation delay, which is, the time consumed by *RSU* to decrypt the received message, get the pointer information and *PID* from the corresponding transaction and generate the challenge message, with encryption using the public key of the *PID*. The communication delay, which totally depends on the increasing number of vehicles, is also shown in Fig. 3. We noted the delay to be around 45ms for up to 5 nodes, but it increases linearly with nodes advancing from 5 to 10. However, witnessing the nature of the two graphs, considering the minimal amount of time in the ECC encryption and decryption, signature generation and verification, querying the ledger, and verifying the outputs, the delay is admissible, with the amount of security it acheives. Thus, we conclude that the slight variation in the two graphs is attributable to these additional steps as depicted in the Fig 4.

D. *Packet-Delivery Ratio(PDR)*

PDR defines the number of packets successfully delivered over the gross packets transmitted. The graph in Fig. 5 shows the comparison of how many packets are delivered successfully before and after application of the framework. The PDR values before encryption shows a linear rise between 90% and 96% with 35 vehicles and further increasing to 98% as number of vehicles move from 35 to 50 vehicles. With our proposed security framework, it is evident from the graph that up to 35 vehicles it is constant at 95%, which starts to drop with increasing traffic on road from 35 to 50 vehicles.

VI. THEORITICAL ANALYSIS

RSU uses Diffie-Hellman key-agreement protocol for key establishment [19], whereas in this paper, *TA* issues public private key-pair for vehicles using ECC, along with IBE scheme for key establishment. The *OBU* when enters the vicinity of a new RSU, sends a message to the *RSU* which is encrypted with the OBU's private key and is then decrypted by the *RSU* using the former's public key in [19]. Whereas, in the proposed framework, the *PID* of vehicle, the transaction id and the block pointer are encrypted with the *RSU's* identity for authentication and the private key of the *RSU* is further used to decrypt and fetch the contents of the message. The proposed algorithm implements traceability using the concept of hash map and pointer to the ledger and revocation by taking the authenticated transaction as the input and spending the received amount, which sets the revocation flag in the revocation transaction to be true. The *CA* updates the status as revocated in the hash map. In [19], authors use a group table for traceability but do not implement revocation. It utilizes the concept of secret keys for message forwarding within the group and hops for communication between the groups. In [19], more time is consumed when the revocation list grows larger.

Issue of the key-pair by the *CA* and storing the corresponding PID_i and certificate on the blockchain, assures two things, firstly, when the vehicle communicates with the RSU with these credentials, by

confirming with the matching transaction on the blockchain *RSU* knows they have not been tampered. Second, it ensures that the vehicles have not been revocated.

A. *Security Analysis*

Our security analysis is based on the following claims where we argue that, justifications to our claims are validated by experimental results obtained through simulation.

Claim-1: Proposed method *reduces the dependency* on *CA* thereby *reducing the communication overhead* in vehicle authentication.

Proof: Unlike traditional methods, whereby the *RSU* communicates with the *CA* for identity or pseudonym verification for every communication, in our case we have eliminated that dependency by introducing a shared ledger. The dependency on the *CA* exists, but only for initial System parameters, key generation and distribution. Unlike traditional methods, the communication overhead is reduced with 'no certificates' in communication.

Claim-2: An *impersonation attack* cannot be launched by an internal or external attacker.

Proof: Our protocol is secured against any impersonation attack, which in turn prevents data tampering of the packets and thus provides integrity of data packets. Since we are using the ECC cryptography, to gain access to user keys, he must be able to solve the ECDLP as discussed in section III.D, which is computationally hard enough to make the system secure. Firstly, an external attacker cannot have block pointer details for authentication and second, the ledger is cryptographically secure.

Claim-3: There is no single point of failure for the actual user data.

Proof: Considering that, each of the *CA*, *RA* and *RSUs* maintain a copy of the authentication and revocation ledger; if one of them loses these copies, then they are easily recovered. The RSUs due to storage crunch might not contain the complete copy at any single time but can access the ledger if required.

VII. Conclusion and Future Directions

This paper presents a novel and efficient technique of mutual authentication in the VANET environment. The framework not only just authenticates vehicles with reduced dependency on the trusted third party but, also preserves their anonymity without revealing the original identity of users. Despite reducing the communication overhead, the framework serves to achieve statutory security requirements. It eliminates the need to circulate CRLs by the *CA* or *RSUs*, and instead mends the status of a vehicle's revocation flag to be true. In future, we would like to decentralize the VANET environment by further exploring the characteristics of the blockchain technology. We aim to use smart contracts particularly and aim to deal with an emergency scenario, which automatically either updates the ledger for nearby *RSUs* or sends an alarm to the nearby vehicles depending on the entries of authenticated vehicle database.

References

[1] U.S. Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety Communications Project—Final Rep., Apr. 2006. [Online]. Available: http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2005/CAMP3scr.pdf

[2] Y. J. Li, "An overview of the DSRC/WAVE technology", In *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness,* 2010, pp. 544-558.

[3] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008)

[4] L. Buttyán, T. Holczer, and I. Vajda. "On the effectiveness of changing pseudonyms to provide location privacy in VANETs", 2007, *ESAS*, vol. 4572, pp 129-141

[5] L. Zhu, C. Chen, X. Wang and A. O. Lim, "SMSS: Symmetric-masquerade security scheme for VANETs." *Autonomous Decentralized Systems (ISADS),* 2011, pp 617-622.

[6] K. Gai, M. Qiu, Z. Xiong, and M. Liu, Privacy-preserving multi-channel communication in Edge-of-Things, Future Generation Computer Systems, 2018, vol 85, pp 190-200.

[7] D. Puthal. "Lattice-modelled Information Flow Control of Big Sensing Data Streams for Smart Health Application." *IEEE Internet of Things Journal* (2018).

[8] K. Gai, and M. Qiu, Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers, IEEE Transactions on Industrial Informatics, 2017.

[9] S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P. H. Huang and M. K. Khan, "Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs" *IEEE Transactions on Vehicular Technology*, 2017, vol, 4, pp 3235-3248.

[10] G. Calandriello, P. Papadimitratos, J. P. Hubaux and A. Lioy, "Efficient and robust pseudonymous authentication in VANET", In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, 2007, pp. 19-28.

[11] I. Memon, Q. Ali, A. Zubedi and F. A. Mangi, "DPMM: dynamic pseudonym-based multiple mix-zones generation for mobile traveler", *Multimedia Tools and Applications*, 2017, *vol* 22, pp 24359-24388.

[12] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das. "Everything You Wanted to Know About the Blockchain." *IEEE Consumer Electronics Magazine*, 2018.

[13] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and C. Yang, The blockchain as a decentralized security framework, *IEEE Consumer Electronics Magazine*, 2018, vol. 2, pp.18-21.

[14] Y. Yuan, and F. Y. Wang, "Towards Blockchain-based Intelligent Transportation Systems," *In 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2016,* pp. 2663-2668.

[15] S. Rowan, M. Clear, M. Gerla, M. Huggard and C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels", 2017, arXiv preprint arXiv:1704.02553.

[16] P. technologies, Proof of authority chains (2017). URL https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains.

[17] C. T. Li, M. S. Hwang and Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks." *Computer Communications*, *vol* 12, pp 2803-2814,2008.

[18] http://veins.car2x.org

[19] K. Lim, and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks", *Vehicular Communications*, 2016, vol 4, pp.30-37.