Efficient Distributed Admission and Revocation using Blockchain for Cooperative ITS

Noureddine Lasla*, Mohamed Younis§, Wassim Znaidi* and Dhafer Ben Arbia*
*Qatar Mobility Innovations Center (QMIC), QSTP, Doha, Qatar
Email: noureddinel,wassimz,dhafera@qmic.com
§ Univ. of Maryland, Baltimore County, Baltimore, MD, USA
Email:younis@umbc.edu

***Abstract*—Cooperative Intelligent Transportation System (C-ITS) enables inter-networking of vehicles for alerts exchanging in order to improve road safety. While this technology is about to enter the market in the upcoming years, critical questions related to the communication security continue to be challenging research concerns. Current solutions to secure inter-vehicle communication depend mainly on the use of digital certificates for authentication. However, such an approach imposes significant overhead on vehicles since it is computationally demanding and requires validation of the certificate within a limited period. In addition, relying on a central node for deciding on issuing and revoking certificates introduces a single point of failure and could even risk the safety of motorists. In this paper, we propose the use of Blockchain to keep track of the certificate of each vehicle (valid or revoked) in distributed and immutable records. In essence we replace certificate verification with a lightweight blockchain-based authentication approach. In addition, we propose a fully distributed vehicle admission/revocation scheme. We show that our scheme could alleviate the computation overhead and enhance the response time while improving the overall system security.**

I. Introduction

Vehicles in C-ITS periodically broadcast safety messages to their neighbors informing about their surroundings and warning drivers of possible incidents. The significant impact of Vehicle-to-Vehicle (V2V) communication on road safety motivates security provisioning to safeguard the network against foul plays. The conventional method to ensure security is to digitally sign each safety message and control membership of vehicles in the system by applying authentication protocol to certify the identity of participants, where a certificate is issued at the time a vehicle joins the system. Each safety message is signed using the vehicles private key and includes its digital certificate. Any receiver has then to check the signature to ensure message integrity and verify the certificate to authenticate the sender.

The ETSI TS and IEEE 1609.2 standards recommend the use of a Public-Key Infrastructure (PKI) with a centralized management for the creation, distribution and revocation of the digital certificates. Typically, a PKI is mainly based on Certificate Authority (CA) that acts as a trusted third party to issue/revoke digital certificates. However, the use of a CA introduces a single point of failure in the C-ITS. Indeed, dramatic consequences could be caused when the CA is compromised. Over the last decade, several cyber-security attacks have been launched against CA networks [7], [10] resulting into breaches; the inflicted damage includes hacking user accounts, issuing fake certificates and carrying out successful man-in-the-middle attacks [10]. Moreover, the inclusion of the certificate does not only introduce major computation overhead for performing the verification procedure but also imposes high communication overhead in terms of bandwidth. Additionally, it causes increased medium access contention and consequently longer message delivery delays [4], [5]. Basically, in order to include a certificate in a CAM or BSM packet (safety messages defined by ETSI TS and IEEE 1609.2 standards, respectively) additional 145 bytes are required. Several studies have been conducted to quantify the security overhead and to assess its impact on safety applications [12], [16]. For instance, in [16] the impact of the signature and certificate verification on the braking distance has been analyzed; the analysis has shown that the distance can increase by more than an average length of a vehicle during heavy traffic.

To overcome the above mentioned shortcomings, several schemes have been proposed; most of these schemes have focused on reducing the computation and communication overheads and only very few of them have considered the single point of failure vulnerability. In this paper, we opt to overcome the shortcomings of existing solutions using the Blockchain technology.

Blockchain is one of the most revolutionizing technology that can tremendously influence the future of various computer and communication systems [19]. Blockchain provides a secure shared database, ledger or log of transactions, without requiring a central trusted party for its management. The consistency of the blockchain is guaranteed through a distributed consensus protocol where a set of participants (validators), in a trust-less peer-to-peer network, collaborate in a completely transparent way to accept only valid transactions. By design, every transaction is cryptographically encoded into a permanent record and it is almost impossible to modify any of them without being detected [3]. The full history of all performed transactions can be easily retrieved and checked by any entity in the network without additional security mechanisms.

In this paper, we propose the use of blockchain as a mean to keep track of the status of vehicle's membership, i.e., valid or revoked, in order to: (i) mitigate the single point of failure (central authority) vulnerability, and (ii) reduce the overhead

978-1-5386-3662-6/18/$31.00 ©2018 IEEE

of the authentication process (certificates exchanges and verification). In our proposed system, the admission/revocation of vehicles is performed in a completely distributed fashion. A set of blockchain validators, e.g., road side units, apply a distributed consensus protocol to decide about the admission/revocation of a vehicle based on a set of predefined rules.

Because the integrity and validity of the vehicle state information in the blockchain is ensured and can be simply and securely accessed from anywhere, vehicles no longer need to include a certificate in their safety message for authentication. To authenticate a sender of a safety message, the receiver can simply check if the sender's public key used to sign the message is already recorded in the blockchain with a valid status. This considerably reduces both the communication and computation overheads associated with the use of certificates.

The remaining of this paper is organized as follows. Section II provides a summary of the related work. Section III describes our proposed blockchain-based authentication scheme for C-ITS in detail. In Section IV, we discuss the system efficiency and evaluate its performances in comparison to traditional systems. Finally, Section V concludes the paper.

II. Related Work

Alleviating Verification Overhead: To address the concern about the certificate verification overhead, several classes of solutions have been proposed. Some approaches have focused on minimizing the certificate overhead [5], [8], [9], [18]. The optimization methodology can be classified into three categories; Periodic certificate omission [5], neighbor-based certificate omission [18] and congestion-based certificate omission [8], [9]. Although excluding certificates in some messages reduce the medium access contention and message delivery delay, it leaves the system vulnerable to security attacks during the certificate omission periods.

Another approach is to apply a lightweight scheme for authenticating safety messages or senders, that were previously authenticated using certificates. For example, in [2], the authors use the physical layer characteristics as a means to authenticate upcoming messages from a sender that has a valid certificate which was previously verified. By assuming that a wireless link between a particular pair of sender and receiver has a unique physical signature, the receiver needs to verify the sender's certificate only once, and all subsequent messages will be automatically accepted until the end of the session. For this scheme to work correctly, however, the wireless channel must be stable, unique, measurable and unspoofable, which is not often the case in a highly dense vehicular network.

In order to completely avoid certificate verification, Bloom Filters (BFs) have been applied in [13]. BFs are generally used to make inexpensive lookups or membership checking with relatively very low false positive rates [15]. Although this scheme could reduce the overall computation complexity for the verification, it still needs to incorporate the certificate within each CAM message and to also perform the verification when suspecting a false certificate.

Blockchains Use in ITS: Recent years have witnessed growing interest in the application of the blockchain technology in C-ITS [21], [17], [6], [14]. In [21], a seven-layer conceptual model for blockchain-based ITS has been proposed and its potential utility in parallel management transportation system has been highlighted in [20]. In [6] a blockchain-based architecture for ITS is proposed to ensure privacy in situations where vehicles are connected to the Internet. Examples include wireless remote software update, car insurance and smart charging services. However, very few studies have considered the problem of securing vehicle-to-vehicle communication using blockchain [14], [17]. The work in [14] have proposed the use of blockchain to improve the efficiency of group key management schemes used to secure group broadcast within heterogeneous vehicular network. The blockchain is mainly used to simplify and improve the distribution of the group keys in situation where different security domains exist and, traditionally, belong to different security managers. Another study [17] has examined the use of blockchain for securing inter-vehicular communication through visual and ultrasonic side-channels. Basically, a session key establishment protocol has been proposed relying on both, side channels and blockchain infrastructure. To the best of our knowledge, no prior work has exploited blockchains in providing lightweight security services for VANET while avoiding the presence of a single point of system failure.

III. Efficient authentication for C-ITS

In this paper we propose a new blockchain-based authentication mechanism for inter-vehicles communication. The design objective is to eliminate the single point of failure and reduce the communication and verification overheads which exist in the PKI while ensuring authentication. To achieve such objective, the blockchain-based authentication mechanism for C-ITS has to ensure the following mandatory set of functionalities:

1) Registering the public key of a vehicle;
2) Validating the membership of a vehicle's public key;
3) Looking up/verifying the validity of a vehicle's public key;
4) Revoking a vehicle's public key from the network;

The detailed description of these functionalities implementation is given in the balance of this section. Before that, we first provide an overview of our proposed system.

A. System overview

Our goal is to enable large scale deployment of a vehicular network while preserving its security. Current ITS standards promote the use of PKI with a centralized certification authority to ensure integrity, authentication and non-repudiation. However, such approach introduces a single point of failure and imposes heavy cost in terms of computation and communication overhead, which negatively affects the network performances. Our proposed system leverages the use of blockchain technology to tackle these issues. Intrinsically, blockchain provides a distributed, secure and immutable records of any kind

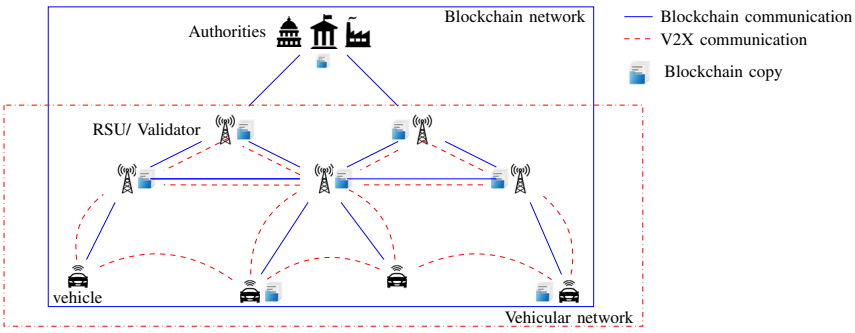

Fig. 1. Blockchain within a vehicular network: RSUs are validators (read/write permissions), whereas authorities and vehicles can only read or send transactions to RSUs for validation.

of data. When putting the authentication information, such as certificates, on blockchain, exchanging and verifying such information becomes unnecessary. In addition, the distribution nature of blockchain eliminates the need of a trusted third party to manage and secure data, which leads to avoiding the single point of failure scenario and averting serious cyber threats (i.e., DoS attacks), which are possible in conventional PKI-based systems.

Figure 1 shows a general architecture of our system where the blockchain network is overlaid on top of the existing vehicular network. In our proposed system, information about vehicle admission/revocation are posted to a permissioned blockchain, where we refer to the entities writing such information as "validators". Thus, we eliminate the single point of failure by delegating decisions about vehicles admission/revocation to a set of validators. We assign the validation role to the Road Side Units (RSUs) as they are deployed over the whole road network, easily reachable by vehicles and are generally interconnected by the mean of specialized links. In this permissioned blockchain, both vehicles and authorities can only read from or submit transactions to the blockchain. By executing a distributed consensus algorithm, the validators (i.e., RSUs) decide to accept or reject the received transactions from both vehicles and authorities.

In practice, the role of the authorities, such as the department of motor vehicle, insurance companies, and manufacturers, is to certify that a particular vehicle conforms with membership requirements. However, instead of collecting all certificates from the different authorities into one single place for decision, in our system all certificates are pushed to the blockchain network then used by the validators for decision making in a fully distributed manner. This is very important from a security perspective as there is no single entity controlling the admission of vehicles to the network. In addition, for the revocation process, the decision for evicting a vehicle is to be performed by the set of validators instead of a single authority. A vehicle that detects misbehavior sends an embedded notification within the transaction to the blockchain, then the final decision about revoking a suspected vehicle is taken by the set of validators following some predefined rules. The admission/revocation information recorded in the blockchain are used by vehicles to authenticate each other with a minimum communication and computation overhead. A vehicle no longer needs to append its certificate to each safety message and the receiver has only to make a simple lookup to check if the sender has an entry in the blockchain with a valid status.

B. Vehicle registration

Before a vehicle v_i can join the network it needs first to generate a public-private key pair (pk_{v_i}, sk_{v_i}), where the private key is kept secret and used to sign safety messages sent by v_i. The public key of v_i is made known to other vehicles and is used by message recipients to verify message integrity, to authenticate the sender, and to check the membership status of v_i on the blockchain. To have a valid membership status on the blockchain, v_i needs to get enrollment certificates from corresponding authorities. Each authority a_j using its private key sk_{a_j} can issue a signed certificate to v_i if it is eligible (e.g., v_i has a valid VIN number, v_i is not stolen, etc.). Finally, the obtained certificate is pushed to the blockchain network for validation through a registration transaction. The certificates are pushed by the according authorities and the transaction has the following format: $< cert,\ registered,\ sig(sk_{a_j}, cert) >$, where $cert$ is the generated certificate by the authority a_j, and sig is the signature of the certificate using sk_{a_j}. Mainly, the certificate contains the public key of the vehicle and the validity period.

C. Vehicle admission

The blockchain network consists of a set of validators, $M = \{m_1, m_2, .., m_k\}$, that execute a consensus algorithm to reach agreement about the state (authorization) of vehicles. When the blockchain network receives a registration transaction from an authority to authorize a new vehicle, or re-authorize a revoked vehicle, the transaction will be accepted if it comes from an authenticated authority. When a sufficient certificates for a particular vehicle v_i are received, one of the validator will generate a new admission transaction to add and mark the public key of the vehicle as valid in the blockchain. The admission transaction has the following format: $< pk_{v_i},\ valid,\ sig(sk_{m_j}, pk_{v_i}) >$; of course the remaining validators will first check the correctness of the

transaction before adding it to their local blockchain copy. The verification mainly consists of checking the validator's signature and that the concerned vehicle has sufficient certificates (registration transactions) on the blockchain.

D. Vehicle authentication

Once a particular vehicle v_i is added and labeled in the blockchain as valid, it can join the network and start sending safety messages. To ensure massage integrity, the sender still needs to sign the message using its private key. Therefore, each vehicle that receives a message from v_i needs, first, to authenticate the sender by simply checking if the public key of v_i, that corresponds to the private key used to sign the message, exists in the blockchain and is marked as valid. Second, the receiver checks the integrity of the message by verifying its signature using the public key of v_i. In contrast to the traditional PKI-based system, where the sender and the receiver have to include and verify a digital certificate, respectively, in our system the certificate is no longer included in the safety messages and the certificate verification is replaced by a simple lookup function. The lookup function is much more faster than the cryptographic signature verification of the certificate. This will considerably increase the performance of the system and improve the timeliness of incident announcements. A comparison between the lookup and the signature verification speed is given in Section IV.

E. Vehicle revocation

To enable a distributed revocation process, each vehicle v_j that detects misbehavior of v_i has to send a misbehavior transaction to notify the blockchain network. The misbehavior transaction has the following format: $< pk_{v_i},\ misbehavior,\ sig(sk_{v_j}, pk_{v_i}) >$, where pk_{v_i} is the public key of the suspected vehicle and sk_{v_j} is the private key of the vehicle that report the misbehavior. The validators will accept and add these transactions to the blockchain if they are originated from valid vehicles. These transactions will be later collectively considered to decide about whether revoking the membership of v_i is warranted.

In order to revoke a suspected vehicle, a distributed revocation protocol will be executed by the blockchain validators. The revocation is generally based on rules set by a high authority and enforced by the validators. For instance, the validators can decide to revoke a particular vehicle v_i if more than n authentic misbehavior transactions for v_i are added to the blockchain in the past 24 hours. If v_i is to be evicted from the network, one of the validator will create a revocation transaction and broadcast it to the blockchain network. The revocation transaction has the following format: $< pk_{v_i},\ revoked,\ sig(sk_{m_j}, pk_{v_i}) >$, where pk_{v_i} is the public key of the vehicle to be evicted and sk_{m_j} is the private key of the validator. Once receiving the revocation transaction, the other validators will add it to the blockchain after checking the authenticity of its source.

TABLE I
SUMMARY OF THE SET OF USED TRANSACTIONS

Transaction type	Sender	Transaction
Registration	Authorities	$< cert,\ registerd,\ sig(sk_{a_j}, cert) >$
Admission	Validators	$< pk_{v_i},\ valid,\ sig(sk_{m_j}, pk_{v_i}) >$
Misbehavior	Vehicles	$< pk_{v_i},\ misbehavior,\ sig(sk_{v_j}, pk_{v_i}) >$
Revocation	Validators	$< pk_{v_i},\ revoked,\ sig(sk_{m_j}, pk_{v_i}) >$

A summary of the different transactions used by our system is given in Table I.

IV. DISCUSSION

A. Storage Requirement and Optimization

The number of transactions on the blockchain is proportional to the number of vehicles and revocation/re-registration events, which could be very large. For instance, according to the European Automobile Manufacturers Association (ACEA) [1], the number of vehicles on the Europe road in 2017 is more than 250 million. This make the size of the blockchain a big issue for devices with limited storage capability, such as the On-Board Unit (OBU) used by vehicles to communicate with each others and with RSUs. To mitigate to this issue the following techniques are suggested:

1) Multiple blockchains: Instead of having only one blockchain that holds the different information related to vehicle registration, admission, misbehavior and revocation, each type of data can be stored in a distinct blockchain. In this case, vehicles will use only the admission and revocation blockchains as they are sufficient to authenticate the source of any received safety message. Therefore, a considerably memory space can be saved.

2) Pruning: An intuitive approach to decrease the size of the blockchain is to remove useless information. For instance, entries about old vehicles that are already revoked can be removed from the vehicle's copy of the blockchain. The same applies for the admission transactions of vehicles that are already revoked. Note here that useless transactions can be only removed from vehicles' copy, and are entirely preserved in validator node to ensure blockchain security.

3) Cryptographic accumulator: Another technique for optimizing the blockchain storage is by using cryptographic accumulator. As discussed in [11], the idea is to accumulate the set of valid vehicles into one single digital object, where each vehicle v_j will have a membership witness to prove that v_j is already registered in the accumulator. In this case, only the accumulator will be saved on the blockchain, and vehicles have only to include their witness in their safety messages in order to allow the receiver to check the membership by applying a simple function. This will considerably decrease the size of the blockchain and can scale for very large network sizes without affecting the storage performance.

B. Verification performance

By using a blockchain, the authentication of a vehicular safety message turn into a simple lookup to find whether the sender's public key exists with a valid status. In order

TABLE II
EXPERIMENTATION SETUP

CPU	4 x Intel(R) Core(TM) i5-2520M @ 2.50GHz
CPU-cache	3072 KB
LevelDB	Version 1.9
Number of transactions	18 164 497

to evaluate the verification time when using our scheme and compare it to the signature verification of digital certificate in conventional PKI, we have conducted the following experiment. To test the lookup function on a real scenario, we selected the Bitcoin blockchain as it is the largest existing one with millions of transaction entries. In Bitcoin, to speedup access and search operations, the levelDB database is used [3]. Bitcoin uses mainly two databases, the first one contains metadata about all known blocks and their location on disk. The second database contains a compact representation of all currently unspent transaction outputs (UTXO), in order to make it easier to validate a transaction for redeeming some bitcoins. It is worth noting that the database scheme can be customized to fit a specific requirement. In our experiment we calculated the response time when searching for a particular transaction in the blockchain database. By using Plyvel, a python interface to levelDB, we can access directly to the database and then search for a particular transaction by its identifier (TXID). Several queries have been issued in the experiments and the response time has been averaged. A summary of the used database and the hardware setup for the experiment is given in Table II.

The result, by averaging 1000 queries, shows that the average required time to lookup for a transaction is about $0.012ms$. Whereas, when verifying a digital signature, by executing the program `"openssl speed ecdsa"` which gives the verification time of the ECDSA, the result is about $0.1ms$ for a key size of 256. The advantage of using blockchain in this case is very clear as the verification delay is nearly dropped by a factor of 10.

V. CONCLUSIONS

Using blockchain for securing C-ITS is an efficient alternative to the traditional PKI-based systems. In this paper, we have presented a blockchain-based system for C-ITS, which avoids the presence of a single point of failure and reduces both the communication and computation overhead. Our systems takes advantage of the distributed nature of the blockchain and the immutability of its records to provide a secure and lightweight authentication mechanism for inter-vehicles communication. Our system support vehicle registration, admission, misbehavior notification and revocation in a completely decentralized manner. Moreover, our system design eliminates the inherent heavy computation when verifying digital certificates and enables authentication using a simple lookup function. In summary, we believe that our proposed system is a viable solution that offers better security and performance than existing solutions. In the future, we plan to implement our system and evaluate it performance for various network sizes using contemporary VANET-based simulators.

VI. ACKNOWLEDGEMENT

This paper has been accepted for publication in Blockchains and Smart Contracts workshop (BSC'2018).

This paper was made possible by NPRP grant #[7-1113-1-199] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] Vehicles in use - europe, 2017. http://www.acea.be/statistics/article/vehicles-in-use-europe-2017.

[2] Ala'a Al-Momani, Frank Kargl, and Christian Waldschmidt. Physical layer-based message authentication in vanets. In *Fachgesprch Inter-Vehicle Communication 2016*, pages 14–17, 2016.

[3] Andreas M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Crypto-Currencies*. O'Reilly Media, Inc., 1st edition, 2014.

[4] S. Bittl, K. Roscher, and A. A. Gonzalez. Security overhead and its impact in vanets. In *2015 8th IFIP Wireless and Mobile Networking Conference (WMNC)*, pages 192–199, Oct 2015.

[5] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy. On the performance of secure vehicular communication systems. *IEEE Transactions on Dependable and Secure Comp.*, 8(6):898–912, 2011.

[6] Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak. Blockchain: A distributed solution to automotive security and privacy. *CoRR*, abs/1704.00073, 2017.

[7] Tom Espiner. Trustwave sold root certificate for surveillance. 2012.

[8] M. Feiri, J. Petit, and F. Kargl. Congestion-based certificate omission in vanets. In *ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*, VANET '12, pages 135–138, 2012.

[9] M. Feiri, J. Petit, and F. Kargl. Evaluation of congestion-based certificate omission in vanets. In *IEEE Vehicular Networking Conference (VNC)*, pages 101–108, Nov 2012.

[10] Dennis Fisher. Final report on diginotar hack shows total compromise of ca servers. 2012.

[11] Conner Fromknecht, Dragos Velicanu, and Sophia Yakoub. Certcoin: A namecoin based decentralized authentication system. MIT project 2014.

[12] Muhammad Awais Javed, Elyes Ben Hamida, and Wassim Znaidi. Security in intelligent transport systems for smart cities: From theory to practice. *Sensors*, 16(6), 2016.

[13] Hongyu Jin and Panos Papadimitratos. Bloom filter based certificate validation for vanet: Poster. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '17, pages 273–274, 2017.

[14] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, PP(99):1–1, August 2017.

[15] M. Mitzenmacher. Compressed bloom filters. *IEEE/ACM Transactions on Networking*, 10(5):604–612, Oct 2002.

[16] Jonathan Petit and Zoubir Mammeri. Authentication and consensus overhead in vehicular ad hoc networks. *Telecommunication Systems*, pages 2699–2712, 2013.

[17] Sean Rowan, Michael Clear, Mario Gerla, Meriel Huggard, and Ciarán Mc Goldrick. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. *CoRR*, abs/1704.02553, 2017.

[18] Elmar Schoch and Frank Kargl. On the efficiency of secure beaconing in vanets. In *Proceedings of the Third ACM Conference on Wireless Network Security*, WiSec '10, pages 111–116. ACM, 2010.

[19] Melanie Swan. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[20] F. Y. Wang. Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications. *IEEE Transactions on Intelligent Transportation Systems*, 11(3):630–638, 2010.

[21] Y. Yuan and F. Y. Wang. Towards blockchain-based intelligent transportation systems. In *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pages 2663–2668, Nov 2016.