Secure Blockchain-Based Communication Scheme for Connected Vehicles

Jose Angel Leon Calvo and Rudolf Mathar

Institute for Theoretical Information Technology, RWTH Aachen University Aachen, Germany 52074
Email: {leon, mathar}@ti.rwth-aachen.de

***Abstract*—Autonomous connected vehicles are a main concept in the future of Intelligent Transportation Systems (ITS) since they provide an increase in safety and road efficiency. The management and coordination of the connected vehicles is based on periodic communications among the vehicles involved in the network, and with their surrounding environment. However, a major concern regarding this information sharing process is how to provide a secure transmission while fulfilling the latency requirements. Here we propose the use of a joint paradigm to securely manage the inter-vehicular communications. First, a ring-signature based scheme is applied to verify the identity of the vehicles joining the network. Second, the information is shared among the vehicles and consensually verified using a blockchain-based mechanism using secure communication channels created by multi-party smart contracts. The proposed protocol fulfills the stringent requirements in latency for vehicular networks by means of almost instantaneous communications while providing an anonymous secure system for the members of the network relying on cryptographic primitives.**

I. Introduction

Intelligent Transportation Systems (ITS) are gaining momentum as one of the cornerstone fields for the next 5G technology revolution [1]. In particular, autonomous vehicles, i.e., without human interaction in the system, attract most of the attention. In order to provide a feasible autonomous system, the concept *connected vehicles* has been conceived [2]. This idea covers vehicles equipped with on-board units (OBU) which consists of a set of sensors to perceive the environment, and communication devices to enable information sharing with the rest of vehicles. Using this equipment, the vehicles can communicate with the rest of participants in the network, and with the surrounding environment, leading to cooperative schemes [3].

Among the different approaches suggested to obtain an optimal cooperative scheme, platooning seems to be the most promising idea in terms of efficiency and safety. Platooning systems require low latency ($\approx$ 10 ms) and ultra-reliable communications (99.999%) in order to obtain a feasible coordination scheme. These stringent requirements are pushing the limits of the state-of-the-art communication schemes, forcing the scientific community to search for new ways to fulfill these requirements. However, another important topic which is the focus of the present work is how to secure the wireless communications between the vehicles.

In their paper, Petit and Shladover [4] classify the different potential attacks on automated systems, making a distinction between autonomous vehicles and cooperative systems. Our focus is on the latter, where the vehicles in the platoon share their status vector, i.e., position, velocity and acceleration, encapsulated in cooperative awareness messages (CAM) with the rest of participants. The data in these messages are the main information needed to adjust the behavior of the vehicles inside the platoon, and hence, it is the main entry point of potential attacks. Our paper focuses on two different types of attacks: i) non-authorized vehicle joining the platoon, and ii) fake/poisoning the vehicular communications inside the platoon. Thus, we can classify the threats as *attacks from the outside* (the adversary does not have a legitimate cryptographic key and certificate) and *attacks from the inside* (the adversary somehow obtained a legitimate cryptographic key and certificate). Some examples of these attacks are:

- *Unauthorized participation*: unauthorized users act as a legitimate user to participate in the system, and affect the management of the system.
- *Replay attack*: the adversary replicates messages that were sent previously. It may avoid the authentication mechanism and disturb the system. A simple solution is to include timestamps into the messages. However, it adds more computational effort to the network and requires synchronization.
- *Sibyl attacks*: the adversary may try to spread false messages or misleading information to the rest of participants. Once the attacker is validated in the system, it makes the receivers believe that the message is coming from an authenticated source and the content of the message is legit.

Each of those attacks has several direct consequences, and therefore, different mitigation techniques [4]. However, we propose in this work a joint paradigm based on ring-based signatures to invalidate unauthorized participation, along with a combination of blockchains and smart contracts to eliminate replay and sibyl attacks.

The first concept includes the ring-based signatures introduced by Rivest, Shamir and Tauman in [5]. It takes a group of signers $\mathcal{X}$ (in our case the platoon members) without a group manager (unlike group signatures [6]), and allows every group member $\mathcal{X}_i \in \mathcal{X}, i = \{1, \dots, N\}$ to share messages within the group by signing them using the group public key $P_{\mathcal{X}} := \{P_1, \dots, P_N\}$ and its own private key $S_{\mathcal{X}_i} := S_i$. This signature scheme does not require setup procedures, group manager or external coordination between the vehicles, which makes it suitable for fast moving environments as proposed in [7]. However, in the traditional scheme defined before, the signer can send messages without any prior verification by the group or platoon. This is not suitable for our scheme

9781538614785/18/$31.00 © 2018 IEEE

where a potential attacker can overload the network by sending multiple messages (e.g., denial of service (DoS) attack), and congestion is a particularly pernicious consequence in time-critical applications, such as vehicular ones. Thus, we propose a consensus-based scheme in order to accept messages from a new vehicle joining the platoon, i.e., authorization scheme. This feature is explained in depth in Section. III-A.

The second part of our scheme relies on the blockchain technology which was first introduced in the famous Satoshi paper [8]. The blockchain technology is defined as a digital ledger where all the transactions are recorded and publicly announced. Moreover, it uses a chained hash mechanism to make infeasible, i.e., computationally too costly, to modify previously accepted transactions. In vehicular networks, once the vehicles are forming a platoon, it is necessary to secure the inter-vehicular communications. Hence using the blockchain distributed public ledger is possible to validate these messages as shown in [9] applying a consensus-rule. However, one open question pointed in this paper is the excessive time to validate the messages in the blockchain technology, since it needs to be validated by most of the users. Using as reference the Bitcoin cryptocurrency (highest computational power), it takes an average of approximately 10 minutes to validate each transaction which is obviously unacceptable for our time-critical application. Therefore, we need to propose a modification of the standard blockchain transaction.

The standard blockchain protocol has the great advantage of a decentralized validation architecture, i.e., there is no need for a trusted third party authority to work as a referee. However, at the same time it is a great barrier to obtain extremely fast transactions since they need to be accepted by at least 51% of the network members. Therefore, we propose in this case the use of microtransactions. The idea of microtransactions relays in the creation of a relationship between two parties (by means of a smart contract), and to only publish in the blockchain whenever there is a disagreement between both parties, or to publish a single transaction covering all the transactions occurred during a stipulated period of time. The smart contract concept along with the blockchain technology has the following advantages: i) Decentralized: there is no need to rely on an intermediary to confirm the transactions. ii) Safety: since we are using a blockchain scheme, all the transaction are *carved* on a shared ledger, so there is no way to modify the values. iii) Backup: on the blockchain concept, every single participant has a local copy of the last valid blockchain. Nevertheless, storing the complete blockchain is not feasible due to scalability and hardware restrictions of the OBUs. Therein, a widely used concept is to utilize a Merkle tree which summarizes all the transactions in the blockchain by producing a digital fingerprint.

The remainder of this paper is organized as follows. Section II introduces the system model along with the platoon cooperative communication scheme. Section III shows the main contribution of this paper, where the safety mechanisms are defined based on cryptographic primitives. In Section IV, a conclusion is given identifying the main benefits of our approach.

II. System Model

Definitions: we call a set of possible signers a ring $\mathcal{X}$. Each possible signer $\mathcal{X}_i$ is associated with a public key P_i

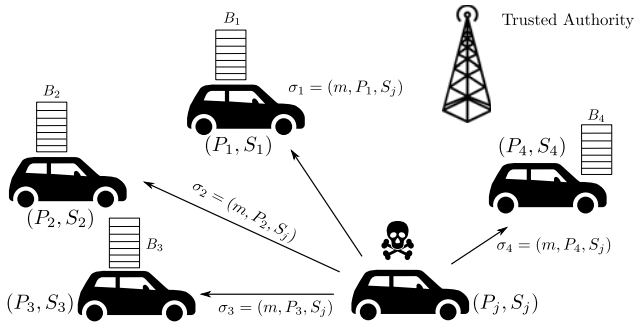

Fig. 1. Adversary trying to join a platoon.

(by means of a public key infrastructure (PKI) scheme) that defines the signature scheme and specifies its verification key. Moreover, the adversarial entity j is defined by its public and private key as (P_j, S_j). Therefore, the ring-signature is defined as $\sigma := (m, P_1, \ldots, P_N, s, S_j)$ which produces the general ring signature σ for the message m given the public keys $\{P_1, \ldots, P_N\}$ of the N ring members and the adversary j. The ring-verification protocol (m, σ) accepts a message m and a signature σ which includes the public keys $\{P_1, \ldots, P_N\}$ of all the members.

Problem statement: create a secure and anonymous scheme for vehicles to join the platoon formation, and for the platoon members to periodically exchange messages using secure vehicle-to-vehicle communications with stringent latency requirements.

Let the system model be defined using a typical vehicular network based on the 3GPP Rel. 14 (LTE-V2X) implementation [10]. The network consists on a set of vehicles $\mathcal{X}$ forming a platoon, and an infrastructure playing the role of a trusted authority (TA) as shown in Fig. 1. Using the RSA cryptosystem (it can also be applied using elliptic curve equivalents) for each vehicle $\mathcal{X}_i$ in the ring $\mathcal{X}$, its public key can be defined as $P_i = (n_i, e_i)$ which specifies the trap-door one way permutation f_i of $\mathbb{Z}_p$ as

$$f_i(x) = x^{e_i} \pmod{p} \tag{1}$$

where we assume that only the vehicle $\mathcal{X}_i$ knows how to compute the inverse permutation f_i^{-1} efficiently. Each vehicle $\mathcal{X}_i$ has an identity defined as $m_i = (I_i || R_i)$ where $||$ denotes concatenation. The identity m_i is created using a permanent vehicle ID, I_i, where one possibility is to use the physical license plate or a virtual one as suggested in [9], and a session salt R_i. This identity m_i is secured using a hash function (typically SHA-256) obtaining the value $k_i = h(m_i)$ which has the property of being preimage resistant, i.e., it is infeasible to find a value y such that $y = k_i = h(m_i)$ providing the desired anonymity to our scheme.

However, there are some open questions regarding our system model: Why do we want to organize the vehicles in platoons? What are the potential attacks to platoon formations? The concept of platooning systems has been brought up to increase the lane capacity and a representation of these systems is depicted in Fig. 2, where Δd and ΔD are the inter-vehicular distance and inter-platoon distance, respectively [11]. In order to manage a platoon, it is necessary to share the vehicle status using wireless vehicle-to-vehicle (V2V) communication, and

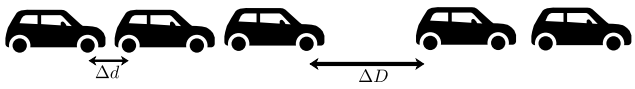

Fig. 2. Optimal Platoon Formation.

here is where the potential cyberattacks may appear. Once the trusted platoon member (one vehicle already in the platoon) receives the signed message (k_j, σ_i) the protocol continues as follows: if the vehicle j is accepted in the platoon (validated by the rest of vehicles using the ring-based signature), the communication between the vehicles is periodic and requires low delay [10]. Therefore, we need to find a secure and almost instantaneous communication scheme (including cryptographic security). For this purpose, we propose to use a blockchain-based protocol. In the normal standard blockchain validation, every single transaction is published and broadcast, and it usually takes an average of 10 min to obtain the six validations needed to trust a transaction. However, as mentioned before, we require an almost instantaneous protocol and hence, we propose the use of the microtransaction concept using smart contracts between the vehicles. This idea is explained in Section III-C.

III. Proposed Security Scheme

The following figure (Fig. 3) describes the general idea regarding the proposed design. It is divided in three different phases involving the vehicles and the trusted authority as shown in Fig.1: i) A ring-based signature scheme to verify the identity of vehicle j and join the platoon. ii) Establishment of a smart contract between the vehicles in the platoon to create secure channels for the microtransactions. iii) Use a blockchain scheme to validate or reject the microtransactions (CAM messages) inside the secure channels.

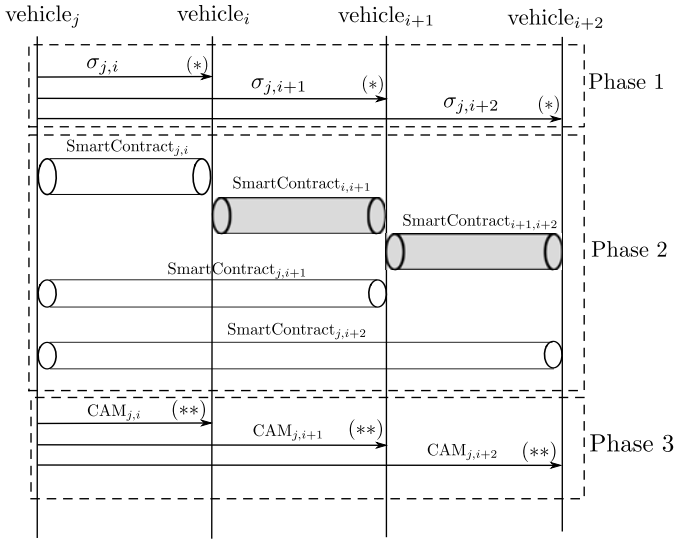

Fig. 3. General flowchart for the proposed scheme

$(*)$ verify the identity of the vehicle j using the TA $(**)$ certify the information sent by vehicle j comparing the values with the readings obtained from the own on-board equipment and the history of values. In the case of a disagreement between the received and read values, the receiver sends the values to the blockchain, so everyone in the platoon can validate or discard the values (51 % rule). Every phase of the proposed scheme is described below in detail.

A. Ring-based Signature for Platoon Joining

1) Ring-signature generation: Let a vehicle j with a pair of keys (P_j, S_j) that wants to join an already formed platoon with N vehicles in it. Each of the vehicles have a pair of keys (P_i, S_i) which correspond to the public and private key, respectively. The designated public keys are authenticated employing a public key infrastructure (PKI) protocol using in our case the eNodeB, acting as the TA, which binds the public keys P_i to the identity of the users $\mathcal{X}_i \in \mathcal{X}$. The binding of the vehicle identity occurs once the vehicle is registered in the network, since the different infrastructures share their database. An emerging new approach to solve the use of certificates using the PKI is the use of blockchain technology [12], which provides a distributed ledger for registering the identities, and more importantly provides a solution which cannot be modified from the outside. The vehicles generate an identification value (pseudonym) like:

$$m_i = (I_i || R_i) \tag{2}$$

which is later hashed by $k_i = h(m_i)$ and it is the message used to ask for joining the platoon. The value R_i is denominated as the session salt which usually has a short life cycle. Here we propose to make the session salt expire every time a vehicle leaves a platoon reducing the number of recalculations in the TA database, but providing a safety mechanism against pseudonym linking attacks [13].

2) Ring-signature verification: Joining the platoon is a consensus-based protocol keeping the anonymity of the joining vehicle j and the vehicles $i = \{1, \ldots, N\}$ already in the platoon. For that matter we propose to use the vector $\vec{\sigma} = (\sigma_{j,1}, \sigma_{j,2}, \ldots, \sigma_{j,N})$ as an identification method. Each of these values is calculated as shown in Fig. 1, using $\sigma_{j,i} = (k_j, P_i, S_j)$ which is the identification value between the adversary vehicle j and the platoon vehicle i. The motivation behind this scheme is that vehicle j sends his identity to vehicle i as the designated verifier. This can be easily achieved using the individual ring-signature obtained by $\sigma_{j,i}$. Using this method, the vehicle i knows that the message is coming from the vehicle j (since no third party could have produced this ring signature due to having the value S_j encapsulated), but vehicle i cannot prove to the rest of participants that the message was signed by the vehicle j, since the message could have been created by vehicle i itself. Once all the values $(\sigma_{j,1}, \sigma_{j,2}, \ldots, \sigma_{j,N})$ are shared between the corresponding vehicles and the vehicle j, the vector $(\sigma_{j,1}, \sigma_{j,2}, \ldots, \sigma_{j,N})$ is sent to the trusted authority (TA). Here we can face two different outcomes: i) if k_j is stored in the TA database then the vehicle j can join the platoon. ii) if $k_j \notin \mathcal{K}$ where $\mathcal{K}$ contains all the valid hashed identities then the vehicle is consider as an adversary. Its identity is published in the blockchain and broadcast, since we know the identity (P_k, S_k), and we can then proceed to repulse the vehicle from the network.
The aim of publishing the identity in the blockchain is twofold: first, the message is received and verified by every vehicle in the platoon, and second, it is computationally impossible to override the values already stored and validated in the blockchain. Moreover, since the blockchain is based on

chained hash operations, the revoked identity is persistent in time.

B. Smart Contracts

Once the vehicle is accepted, it needs to establish a smart contract with the rest of platoon participants. A smart contract is defined as an operation that can be permanently executed between two different parties which have a defined agreement [14], [15]. In our scenario, a smart contract between the vehicles in the platoon is particularly suitable due to the periodic nature of the CAM messages and the stringent delay requirements. Smart contracts have the extra advantage of being completely decentralized (it only involves the two parties of the contract), and they are triggered by an event (in our case a timer or the CAM messages sent periodically). Using a network of these microtransaction channels (as shown in Fig. 3) helps making the network more scalable, since every transaction does not require to be broadcast to every single user, but it only involves the parties in the contract. Moreover, creating tunnels using chained channels, it is possible to send messages to every member of the party in a secure and decentralized manner. However, what happens if there is a disagreement between the parties in the smart contract? Here is where the blockchain technology plays a role as explained in next section III-C.

C. Blockchain-based microtransactions

A blockchain scheme for information sharing verification is considered in our model to protect, as means of securing our system from an inside attacker, i.e., the adversary obtained a legitimate key and it is a member of the platoon. Additionally, we assume that the adversary is able to establish contracts with the rest of participants, since the only requirement is to have a validated identity. The general scheme of microtransactions is shown in Fig. 4 using a smart contract involving two vehicles.

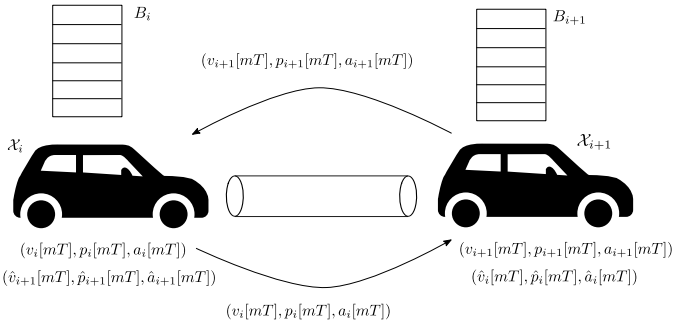

Fig. 4. General microtransaction scheme using blockchain

Using the simple example from Fig. 4 to illustrate our scheme, we have two vehicles $\mathcal{X}_i$ and $\mathcal{X}_{i+1}$, which are self-aware of their own state vector, i.e., position, speed and acceleration. They have established a smart contract, and they have stored a local copy of the blockchain denoted as B_i and B_{i+1}. Moreover, the vehicles can estimate the state vector of the other vehicles in the platoon by means of their on-board sensors. Using the rules established by the smart contract, the microtransacions (CAMs) are triggered every period T (defined as $T = 100$ ms by the standard [10] for vehicular safety applications). Once the vehicle receives the information from the other party, it checks whether its estimates and the received values are similar. In the case of reaching an agreement, i.e., the received information and the estimated values match, the system continues working normally. In the case of having a disagreement, the receiver vehicle raises its discussion to the blockchain, i.e., broadcast the received microtransaction, and the rest of vehicles in the ring, using their own estimate values obtained by their sensors, verify whether the received microtransaction is correct.
Since the vehicles share their state vector every $T = 100$ ms, each vehicles have stored the history of values for the dynamics of each vehicle, and therefore, a prediction about the expected value can be performed as shown in Eq. (3-5). Assume that the velocity of the vehicle does not change in the platoon formation

$$\hat{v}_{i+1}[mT] = v_i[mT] \tag{3}$$

$$\hat{p}_{i+1}[mT] = a_i[mT] + \frac{v_i[mT]}{T} \tag{4}$$

$$\hat{a}_{i+1}[mT] = 0.5\frac{(v_i^2[mT] - v_{i-1}^2[mT])}{v_i[mT] \cdot T} \tag{5}$$

where the predicted acceleration $\hat{a}_{i+1}[mT]$ is calculated using the field measurements obtained from [16]. The requirement of this scheme is to have a synchronized scheme between the vehicles in order to predict and correctly estimate the dynamics of the vehicles. Therefore, two different types of attacks are prevented, i.e., replay and sibyl attacks, are prevented by using the blockchain scheme. The first is a similar concept as the one of double-spending in the Bitcoin network. The vehicles store the received transactions along with a timestamp, where a possible solution for synchronization is using the clock from the GPS system, in order to detect replay attacks. Moreover, since the transactions are published in the blockchain after a period of time, the vehicles can identify if a message has been previously sent. Furthermore, a sibyl attack can be avoided as follows. The blockchain verification of a raised disagreement is based in a consensus-based model, i.e., if the majority of vehicles (51 $\%$ rule) find the value not acceptable, the disagreement is admitted and the vehicle is flagged as an attacker.

D. Scalability and time-critical applications

In order to prove the feasibility of our approach, we compare it with the traditional blockchain scheme. According to the standard blockchain scheme (peer-to-peer network) a majority of nodes in the network has to accept the transaction. Considering a network with N users at least $\frac{N+1}{2}$ users must acknowledge the transaction. Therein, the number of exchanged messages required for each transaction increases as the number of nodes grows. Therefore, we assume that the time to *mine* the hash value of the transaction is t_{hash} and the transmission time between vehicles is t_{TX} along with the time of acknowledging the transaction is t_{ACK}, the total time to accept a transaction is given by

$$t_{\text{transaction}} = t_{\text{hash}} + \frac{(t_{\text{TX}} + t_{\text{ACK}}) \cdot N}{2} \tag{6}$$

Nevertheless, our approach uses microtransactions which upon having a valid smart contract between the parties does not

require the validation of the rest of the network (only when one of the members violates the contract terms). In consequence, the latency requirements can be met since there is no need of waiting for the network acceptance of each transaction. Additionally, our proposed scheme does not suffer from scalability issues since each smart contract is established between a pair of users, and it does not need to be constantly updated.

IV. Conclusion

This paper presents a secure protocol for exchanging inter-vehicular messages which relies on the consensus strength (blockchain). This implementation provides the advantages of being decentralized, anonymous and forgery proof, i.e., the previously accepted values cannot be modified. Additionally, by taking advantage of the proposed platoon formation, which is the optimal one in terms of safety and road efficiency, a ring-based signature scheme is implemented for authentication and to allow the vehicles to join the system. Moreover, the stringent latency requirements in vehicular applications are met by using microtransations to share the information between vehicles, since there is no requirement for constant verification due to the implementation of smart contracts between the parties involved in the system. The proposed system is a perfect candidate for vehicular safety applications owing to its decentralized nature (the TA can be replaced by an authentication scheme based on blockchain). Moreover, since the protocol is dealing with high powered systems users, i.e., vehicles, it is possible to perform moderate costly hash operations for the blockchain verifications.

References

[1] C. Wei, "V2X communication in Europe - From research projects towards standardization and field testing of vehicle communication technology," vol. 55, pp. 3103–3119, 10 2011.

[2] R. Coppola and M. Morisio, "Connected car: Technologies, issues, future trends," *ACM Comput. Surv.*, vol. 49, no. 3, pp. 46:1–46:36, Oct. 2016. [Online]. Available: http://doi.acm.org/10.1145/2971482

[3] R. Hult, G. R. Campos, E. Steinmetz, L. Hammarstrand, P. Falcone, and H. Wymeersch, "Coordination of cooperative autonomous vehicles: Toward safer and more efficient road transportation," *IEEE Signal Processing Magazine*, vol. 33, no. 6, pp. 74–84, Nov 2016.

[4] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, April 2015.

[5] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology — ASIACRYPT 2001*, C. Boyd, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 552–565.

[6] D. Chaum and E. Van Heyst, "Group signatures," in *Advances in CryptologyEUROCRYPT91*. Springer, 1991, pp. 257–265.

[7] Y. Jiang, Y. Ji, and T. Liu, "An Anonymous Communication Scheme based on Ring Signature in VANETs," *ArXiv e-prints*, Oct. 2014.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf."

[9] 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," *CoRR*, vol. abs/1704.02553, 2017. [Online]. Available: http://arxiv.org/abs/1704.02553

[10] 3GPP, "3rd generation partnership project: technical specification group radio access network:study on LTE-based V2X services (release 14)," 2016.

[11] C. Zhang, Y. Zang, J. A. L. Calvo, and R. Mathar, "A novel v2v assisted platooning system: Control scheme and mac layer designs," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Montreal, QC, Canada, Oct. 2017.

[12] C. Fromknecht, D. Velicanu, and S. Yakoubov, "A decentralized public key infrastructure with identity retention," *IACR Cryptology ePrint Archive*, vol. 2014, p. 803, 2014.

[13] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 228–255, Firstquarter 2015.

[14] P. Cuccuru, "Beyond bitcoin: an early overview on smart contracts," *International Journal of Law and Information Technology*, vol. 25, no. 3, pp. 179–195, 2017. [Online]. Available: + http://dx.doi.org/10.1093/ijlit/eax003

[15] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: platforms, applications, and design patterns," *ArXiv e-prints*, Mar. 2017.

[16] J. Xu, W. Lin, X. Wang, and Y.-M. Shao, "Acceleration and deceleration calibration of operating speed prediction models for two-lane mountain highways," *Journal of Transportation Engineering, Part A: Systems*, vol. 143, no. 7, p. 04017024, 2017.