IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 9, 2018, accepted August 4, 2018, date of publication August 7, 2018, date of current version September 7, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2864189

A Privacy-Preserving Trust Model Based on Blockchain for VANETs

ZHAOJUN LU[1], WENCHAO LIU[1], QIAN WANG[2], GANG QU[2], (Senior Member, IEEE), AND ZHENGLIN LIU[1]

[1]School of Optics and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China
[2]Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park, MD 20740, USA

Corresponding author: Zhenglin Liu (liuzhenglin@hust.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant No.61376026.

ABSTRACT The public key infrastructure-based authentication protocol provides basic security services for the vehicular ad hoc networks (VANETs). However, trust and privacy are still open issues due to the unique characteristics of VANETs. It is crucial to prevent internal vehicles from broadcasting forged messages while simultaneously preserving the privacy of vehicles against the tracking attacks. In this paper, we propose a blockchain-based anonymous reputation system (BARS) to establish a privacy-preserving trust model for VANETs. The certificate and revocation transparency is implemented efficiently with the proofs of presence and absence based on the extended blockchain technology. The public keys are used as pseudonyms in communications without any information about real identities for conditional anonymity. In order to prevent the distribution of forged messages, a reputation evaluation algorithm is presented relying on both direct historical interactions and indirect opinions about vehicles. A set of experiments is conducted to evaluate BARS in terms of security, validity, and performance, and the results show that BARS is able to establish a trust model with transparency, conditional anonymity, efficiency, and robustness for VANETs.

INDEX TERMS Vehicular ad-hoc networks, blockchain, trust management, reputation system, privacy.

I. INTRODUCTION

It is estimated that the number of registered vehicles will reach 2 billion within the next 10 to 20 years [1]. Recently, the vehicular ad-hoc networks (VANETs) have been suggested as foundation of the intelligent transportation systems (ITSs) to improve transportation efficiency and ensure safety of both vehicles and pedestrians. Two types of communications, namely the vehicle-to-vehicle (V2V) communication and the vehicles-to-infrastructure (V2I) communication are established in VANETs to promote cooperation among vehicles and to share valuable driving information. Through the dedicated short range communication (DSRC) radio, nearby vehicles exchange messages in V2V and communicate directly with the roadside units (RSUs) in V2I [2].

However, the unique characteristics of VANETs such as high mobility and volatility make it vulnerable to various kinds of attacks. Security, privacy, and trust should be taken into account from the beginning stage of designing VANETs. Although the main security services have been well-studied in other fields that can provide secure communication channels against external attackers, the trust management and privacy issues have become the biggest concerns of people [3]. Specifically, it is fairly difficult to deal with distribution of forged messages from internal vehicles. These forged messages could not only decrease transportation efficiency but also in the worst cases, cause accidental events that can threaten human life [4]. In addition, internal attackers can easily track other vehicles or profile drivers' actions by analyzing all the broadcasted messages in VANETs.

The motivation of this paper is to establish a trust communication environment against internal forged messages while simultaneously preservingwar the identity privacy of vehicles. An effective trust model for VANETs should have the following properties [5]–[7]:

Transparency. Authorities are necessary for VANETs since they are responsible for vehicle registration, network maintenance, and dispute arbitration, etc. However, the activities of authorities should be transparent and under monitoring by all the entities in VANETs.

Conditional anonymity. On the one hand, V2V and V2I communications should be anonymous to preserve the identity privacy of vehicles. On the other hand, anonymity should be conditional to make sure that authorities are able to trace the vehicles in case of disputes.

Efficiency. It should be efficient to determine the authenticity and trustworthiness of an alert message in both congestion and sparsity scenarios.

Robustness. It should be resistant against attackers aiming at deceiving the trustworthiness evaluation or disabling the trust model.

Blockchain is the underlying technology of the Bitcoin protocol that emerged in 2008 [8]. It is a distributed public ledger encrypted using Merkel trees and hash functions and has a consensus mechanism based on a proof of work (PoW) algorithm. These significant features of blockchain make it potential for establishing a desirable trust model in VANETs [9]. All the broadcasted messages and activities of authorities will be written into the immutable and unforgeable ledger, which can be verified and audited by every entity in the network. However, the privacy of nodes was not considered at the time of Bitcoin's original design [10]. By reviewing the ledger, the transactions made with any public key is traceable to a real identity.

In this paper, we propose a privacy-preserving trust model named blockchain-based anonymous reputation system (BARS) to prevent distribution of forged messages while simultaneously preserving the identity privacy of vehicles. The main contributions of BARS are twofold:

First, we exploit the features of a lexicographic Merkle tree to extend the conventional blockchain with an efficient privacy-preserving authentication mechanism. The linkability between the public key and the real identity of a vehicle is eliminated when a certificate authority (CA) operates the certificate issuance and public key revocation. All the activities of CA are recorded in the extended blockchain transparently without revealing sensitive information about vehicles so that public keys can be used as authenticated pseudonyms for communications. A law enforcement authority (LEA) is responsible for managing BARS and storing the pairs of public keys and real identities in case of disputes.

Second, in order to prevent the distribution of forged messages, we design a reputation evaluation algorithm using the reputation score to represent the trustworthiness of messages [11]. All the direct historical interactions and indirect opinions about the senders are recorded in the blockchain as persistent evidence to evaluate the reputation score for each vehicle, which provides an incentive for internal vehicles to share driving information actively and honestly. It is in a distributed and efficient fashion for each vehicle to get the reputation score of any public key that recorded publicly in the blockchain.

The remainder of this paper is organized as follows: Sections II surveys the existing trust models for VANETs. Section III elaborates how to extend the conventional blockchain to achieve efficiency, transparency, conditional anonymity, and robustness. Section IV proposes the anonymous authentication to preserve the privacy of vehicles. The reputation evaluation algorithm is presented in Section V. Then, we conduct a set of experiments in Section VI to evaluate BARS in terms of security, validity, and performance before we finally give the conclusion.

II. TRUST MODELS FOR VANETS

Different from the mobile ad hoc networks (MANETs), several unique characteristics of VANETs make it challenging to design an effective trust model. First of all, high mobility makes it unpractical to build long-term interaction among vehicles. In most cases, two vehicles may exchange a handful of messages just for once. Second, the topology always changes rapidly in VANETs. Thus, a desirable trust model should function efficiently in both congestion and sparsity scenarios Third, attackers would either eavesdrop on the broadcasted messages for vehicles' private information or directly subvert the trust model. It is required that the trust model should be able to resist various attacks and preserve the privacy of vehicles simultaneously.

As shown in Fig. 1, the state-of-the-art trust models can be classified into three categories: (1) the entity-centric trust models, (2) the data-centric trust models, and (3) the combined trust models.

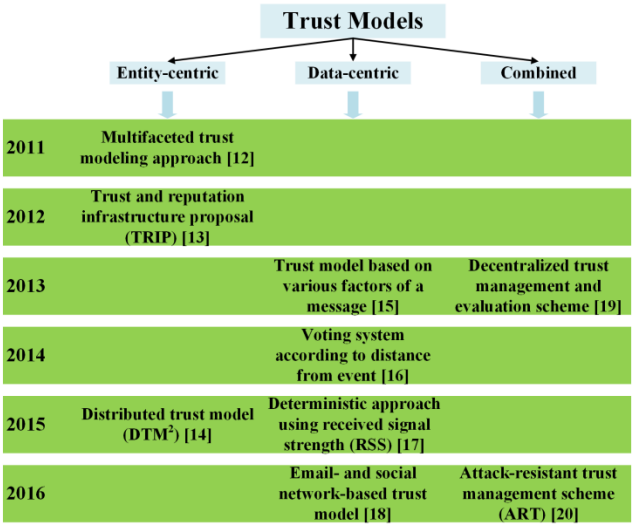


FIGURE 1. Trust models proposed in recent years.

A. ENTITY-CENTRIC TRUST MODELS

The entity-centric trust models focus on evaluating the trustworthiness of vehicles. The main methods to achieve this efficiently and accurately are to establish a reputation system or to make a decision according to the opinions of neighbors. Minhas *et al.* [12] developed a multifaceted trust modeling approach to detect the entities that are generating malicious data. This method incorporates role-, experience-, priority-, and majority-based trust to make a real-time decision. Mármol at al. [13] proposed a trust and reputation infrastructure-based proposal (TRIP) for VANETs to quickly and accurately distinguish the malicious or selfish nodes with the help of RSUs. Haddadou *et al.* [14] proposed a distributed trust model (DTM2) to allocate credits to nodes and securely

manage these credits. Due to the high mobility of vehicles, it is difficult to collect enough information to evaluate the real-time reputation of a specific vehicle. Another serious issue that has not been addressed is how to ensure the security of the reputation system itself.

B. DATA-CENTRIC MODELS

The data-centric trust models focus on the trustworthiness of received data. In order to verify the trustworthiness of received data accurately, the trust models need cooperative information from various sources such as neighbor vehicles or RSUs. Gurung *et al.* [15] proposed a trust model to directly evaluate the trustworthiness of a message based on various factors such as content similarity, content conflict, and route similarity. Huang *et al.* [16] developed a voting system with different voting weights according to its distance from the event. Rawat *et al.* [17] proposed a deterministic approach to measure the trust level of received message by using received signal strength (RSS) for distance calculations as well as the vehicle's position coordinate. Hussain *et al.* [18] suggested an email-based social trust model and a social networks-based trust model to establish and manage the trust level of data. The main drawbacks of the data-centric trust models are latency and data sparsity. Respectively, vast amounts of data from various sources may contain redundant information to incur latency or overwhelm the significant information. On the contrary, since data sparsity is prevalent in VANETs, it is unrealistic for the data-centric trust models to perform well without enough information.

C. COMBINED TRUST MODELS

Both entity and data are the main objects in this category. The combined trust models not only evaluate the trust level of vehicles but also calculate the trustworthiness of data [19]. Thus, these models inherit the benefits and drawbacks of the entity-centric and data-centric trust models. An attack-resistant trust management scheme (ART) proposed by Li and Song [20] coped with malicious vehicles in VANETs. The trustworthiness of data is evaluated based on the received data from multiple vehicles. The trustworthiness of a node is determined based on functional trust and recommendation trust, which respectively indicate whether a node can fulfill its functionality and the trust level of the recommendations from it. The proposed scheme does not take into account the data sparsity, which is pervasive in VANETs.

In order to meet all the requirements of an effective trust model for VANETs, we propose a privacy-preserving trust model managed by semi-trusted authorities. The reputation of each vehicle is evaluated by LEA transparently based on both direct historical interactions and indirect opinions about it. Although the evidence collection and arbitration makes it inevitable to incur delay for the reputation score update process, we believe that it is more essential to make sure that the reputation score can objectively represent the trustworthiness of messages regardless of the density of traffic. Using the extended blockchain technology, the privacy-preserving authentication process is in a distributed and efficient fashion that allows the receiver to get the reputation score of a public key without knowing its real identity.

III. ARCHITECTURE OF BARS

In this section, we first give some necessary assumptions as the foundation of the proposed blockchain-based anonymous reputation system (BARS). Then, we introduce the data structures with the proofs of presence and absence. Finally, we present the main components of BARS, specifically the extended blockchain for VANETs.

A. ASSUMPTIONS

A1. The cryptographic algorithms of the public key infrastructure (PKI) are able to provide secure communication channels between entities as long as the private key is not cracked [21].

A2. The law enforcement authority (LEA) has enough security level to keep the dataset that contains the linkability between the vehicles' public keys and the real identities.

A3. Authorities and RSUs are equipped with customized hardware that has much higher computing power than general-purpose computers.

A4. We assume that it is beyond the adversaries' capability to compromise more than half of vehicles in the network.

Assumption A1 ensures the authenticity and integrity of broadcasted messages. Assumption A2 is the basic requirement for conditional anonymity, which is a trade-off between privacy and security. In case of disputes, it is LEA who has the authority to trace the concerned vehicles for evidence collection. Assumption A3 eliminates the limitations on computing power of authorities and RSUs for data processing, storage, and transmission. Since BARS is built atop of the blockchain technology, assumption A4 is the prerequisite to ensure that the blockchain itself is secure.

B. DATA STRUCTURES

1) CHRONOLOGICAL MERKLE TREE AND PROOF OF PRESENCE

The chronological Merkle tree (CMT) is the underlying data structure of the conventional blockchain [22]. All the transactions (TXs) from authorities are hashed chronologically in CMT and only the root hash is included in the blockchain. Old blocks can then be compacted by stubbing off branches of the tree and the interior hashes do not need to be stored [8].

Fig. 2 illustrates how to efficiently prove that TX_4 is present in CMT. A tuple (Dir, Hash) is enough for the proof of presence for TX_4, in which Dir = {left, left, right} and Hash = $\{Hash_3, Hash_{12}, Hash_{56}\}$. The receiver can calculate the root hash value using the tuple. If this root hash value is equal to that recorded in the blockchain, it means TX_4 is valid.

2) LEXICOGRAPHICAL MERKLE TREE AND PROOF OF ABSENCE

The lexicographical Merkle tree (LMT) regroups all the information about a subject into a single node of the binary

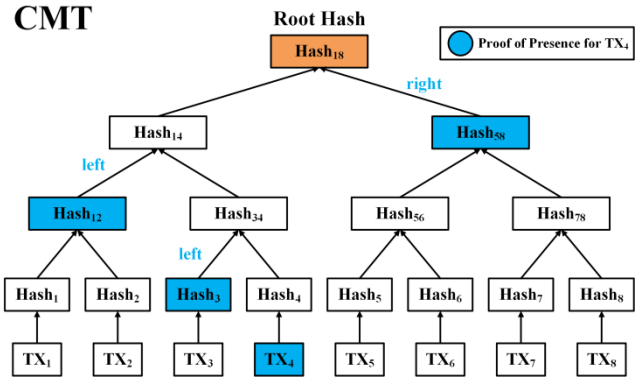


FIGURE 2. Chronological Merkle tree and the proof of presence.

search tree, and while being able to efficiently generate and verify the proof of absence [6]. We consider a total order on bit-strings denoted $\leq$. This order could be the lexicographic order in the ASCII representations but it could be any other total order on bit-strings. LMT is a binary search tree over pairs of bit-strings. For all two pairs (d, h) and (d', h') of bit-strings in LMT, (d, h) occurs in a node left of the occurrence of (d', h') if and only if $d \leq d'$ lexicographically. For all nodes $n \in$ LMT, n is labeled with the pair $(d, H(d||h_l||h_r))$, where d is some bit-string and (d_l, h_l) (resp. (d_r, h_r)) is the label of its left child (resp. right child) if it exists or the constant null otherwise.

As shown in Fig. 3, all the revoked but not expired public keys (PUs) are recorded in LMT. In order to prove that PU_A is not in LMT, one should prove that two adjacent public keys (PU_7, PU_8) exist in the left-right traversal of the tree, meanwhile $PU_7 \leq PU_A \leq PU_8$ lexicographically. A tuple (PU, Hash) is used for the proof of absence, in which $PU = \{PU_7, PU_8, PU_{10}, PU_6\}$ and $Hash = \{h_9, h_{12}, h_4\}$.

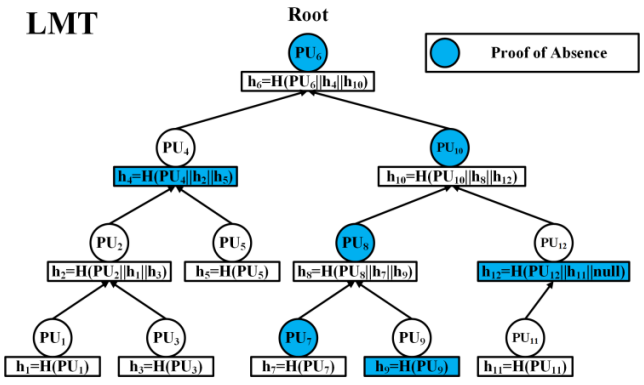


FIGURE 3. Lexicographical Merkle tree and the proof of absence [6].

C. COMPONENTS OF BARS

1) CERTIFICATE

The certificate contains the expiration date, the public key, the signatures of authorities, and the reputation score but no real identity so that the vehicle's privacy is preserved.

2) TRANSACTION

A transaction refers to a message broadcasted by CA to issue a certificate or revoke a public key. Each transaction contains the timestamp and the digital signatures of CA and LEA. Besides, a certificate transaction contains the expiration date and the authorized public key, whereas a revocation transaction contains the revoked public key. In order to preserve the privacy of vehicles, no information linkable to the real identity is included in the transaction.

3) CERTIFICATE AUTHORITY (CA)

CA broadcasts transactions to issue certificates and revoke public keys under the supervision of LEA. All the activities of CA will be recorded transparently and permanently in the blockchain that is public and verifiable to every entity in VANETs.

4) LAW ENFORCEMENT AUTHORITY (LEA)

The main functions of LEA include registration, monitoring behaviors of vehicles, and evaluating the reputation scores of each vehicle. LEA authorizes CA for certificate issuance and public key revocation and keeps the database that contains the linkability between the vehicles' public keys and the real identities with high-level security.

5) ROADSIDE UNIT (RSU)

All the broadcasted messages and transactions are verified by RSUs then will be recorded in the blockchain. Also, RSUs are responsible for updating the data for authentication that stored in each vehicle through V2I communication.

6) VEHICLE

The privacy-preserving authentication scheme among vehicles is running based on the blockchain. On one hand, vehicles can monitor CA and LEA by verifying all the transactions recorded in the blockchain. On the other hand, the global consensus is based on the proof of work (PoW) provided by vehicles. The incentive for vehicles to perform the consensus mechanism is beyond the scope of this paper.

D. BLOCKCHAINS OF BARS

The blockchain is a computational paradigm which emerged with the Bitcoin protocol in 2008 [8]. It is a distributed ledger containing all the transactions ever executed within the network. The ledger is enforced with cryptography and carried out collectively in a peer-to-peer network [23]. As a secure and decentralized computational infrastructure, it is widely acknowledged as a disruptive solution for the problems of centralization, privacy and security when storing, tracking, monitoring, managing and sharing data [9].

There are three blockchains in BARS [24]:

1) BLOCKCHAIN FOR MESSAGES (MesBC)

All the messages broadcasted by vehicles will be recorded in MesBC as persistent evidence for reputation evaluation.

2) BLOCKCHAIN FOR CERTIFICATES (CerBC)

CerBC acts as the public ledger for all the issued certificates. It provides the proof of presence for the sender's certificate with $O(\log^N)$ efficiency. (N is the number of leaves in the Merkle tree)

3) BLOCKCHAIN FOR REVOKED PUBLIC KEYS (RevBC)

RevBC acts as the public ledger for all the revoked public keys. It provides the proof of absence for the sender's public key with $O(\log^N)$ efficiency.

The messages in MesBC and the certificates in CerBC are recorded chronologically in CMTs. Thus, MesBC and CerBC are similar to the conventional blockchain in the Bitcoin. As illustrated in Fig. 4, the RevBC contains a CMT and an LMT. The revoked public keys are recorded lexicographically in an LMT, whose root will change when a newly revoked public key is inserted in it. CMT records the revocation transactions and the corresponding root of LMT chronologically. Only the transaction root of CMT and the public key root of LMT will be stored in the block header. As the consensus mechanism is not the focus of BARS, PoW is adopted and the mining is operated by vehicles.

IV. PRIVACY-PRESERVING AUTHENTICATION

Authentication is to establish the trust between vehicles and has become the most forefront defense for cybersecurity [25]. Several pseudonym updating and exchanging algorithms [26] have been presented to enhance the privacy of vehicles. In BARS, CA and LEA are responsible for three main functions: system initialization, certificate update, and public key revocation. We first introduce the three functions respectively and then explain the process of privacy-preserving authentication.

This paper does not attempt to answer all the questions about certificate issuance and public key revocation, such as under what circumstances a certificate should be issued or a public key should be revoked. BARS provides the ability for every entity to efficiently verify whether a specific public key is revoked and guarantees that the public ledger is consistent across the network, i.e. the certificate and revocation transparency.

A. SYSTEM INITIALIZATION

Initially, each entity generates a pair of private and public keys. When vehicle A enters the network, it uses the secure channel to submit LEA its initial public key and materials to prove its legal identity. LEA will send a signed warrant to CA if the materials are valid. Next, CA will issue an initial certificate to vehicle A.

Note that the submitted materials contain vehicle A's private information. Only LEA preserves them in the database with high-security level, which will be used for tracking the vehicle's real identity in case of disputes.

B. CERTIFICATE UPDATE

Vehicle A will send a certificate update request to LEA in the following cases. First, before the current certificate expires.

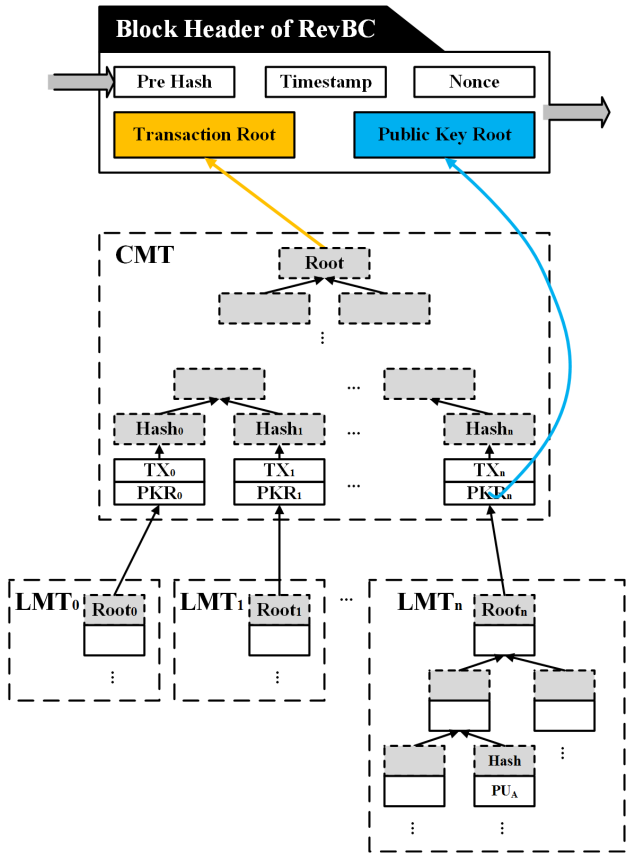


FIGURE 4. Structure of RevBC.

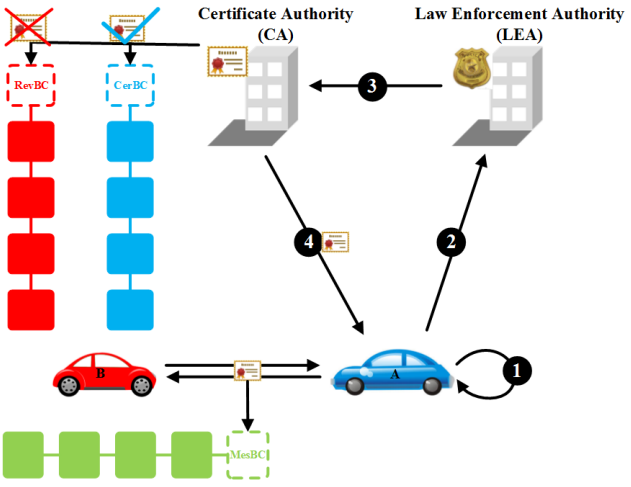


FIGURE 5. Certificate update process.

Second, if the security of its private key is threatened. Third, if it requests to replace its public key for privacy consideration. Vehicle A's public key, reputation score, and expiration date will be updated in a new certificate:

$$C_A^n = \langle PU_{CA}, Sig_{CA}, PU_{LEA}, Sig_{LEA}, PU_A^n, Rpt_A, T_A \rangle \quad (1)$$

Fig. 5 illustrates the steps to update a certificate anonymously.

Step 1: Vehicle A generates a new pair of public key and private key $\{PU_A^n, PR_A^n\}$.

Step 2: Vehicle A sends LEA the certificate update request encrypted with LEA's public key PU_{LEA}. The request includes vehicle A's current public key PU_A^{n-1}, the updated public key PU_A^n, and the signature Sig_A using A's current private key PR_A^{n-1}.

Step 3: If vehicle A's request is verified, LEA will send CA a signed warrant. For the purpose of privacy preserving, the linkability between A's current and updated public key is unknown by CA.

Step 4: CA will verify the signature in the warrant. Then, an updated certificate containing the updated public key PU_A^n, A's reputation score Rpt_A, and the expiration time T_A will be issued to vehicle A publicly and be recorded into CerBC.

C. PUBLIC KEY REVOCATION

$Rev = \langle PU_{CA}, Sig_{CA}, PU_{LEA}, Sig_{LEA}, PU_{rev}, T_{rev} \rangle$ Vehicle A's current public key should be revoked if A's misbehavior is exposed. In order to provide revocation transparency, LEA sends signed revocation warrant to CA that contain the revoked public key PU_{rev} and the revocation time T_{rev}. Then CA broadcasts the revocation transaction that contains the revoked public key, the timestamp, and the signatures of CA and LEA:

RSUs will verify all the revocation transactions, delete the expired public keys, and lexicographically insert the revoked public keys into RevBC.

D. AUTHENTICATION PROCESS

Fig. 6 explains the privacy-preserving authentication process. Vehicle A's certificate C_A is used for authentication. When vehicle B receives C_A, it first checks whether the certificate is expired. If not, B will look up the CerBC and RevBC to make sure that C_A is present in CerBC but PU_A is absent in RevBC, which means PU_A is issued and not revoked by CA. CMT and LMT in the two blockchains provide the proofs of presence and absence with $O(\log^N)$ efficiency. A's privacy is preserved as there is no information about A's real identity in the privacy-preserving authentication process. The security analysis will be presented in Section VI.

V. REPUTATION MANAGEMENT

We present BARS to establish a trusted communication environment for vehicles while simultaneously preserve vehicles' identity privacy. BARS relies on the reputation score of a vehicle to determine the trust level of broadcasted messages. The reputation score gives vehicles the incentive to share safety information and monitor each other so that misbehaviors can be prevented and the distribution of forged messages from internal vehicles can be mitigated. It is an essential issue but out of the scope of this paper to associate the reputation score with a vehicle's actual benefit.

LEA in BARS is responsible for the reputation management based on the authenticity of a broadcasted message as well as its value for other vehicles. The reputation evaluation algorithm should be well-designed to guarantee that:

- The reputation score of vehicle A will increase if A broadcast authentic messages to share safety information with other vehicles. The more significant the safety information is and the more vehicles receive the messages, the more reputation scores A will get.
- The reputation score of vehicle A will decrease if A broadcast forged messages to deceive other vehicles. The more vital the forged messages are and the more vehicles are affected, the more reputation scores A will lose.
- When vehicle A receives forged messages or discovers misbehaviors, A can expose them by submitting evidence to authorities. If A's exposure is true, A's reputation score will increase. But if A lodged a false accusation, A's reputation score will decrease.
- The reputation management is under the monitoring of all the entities in VANETs.

LEA collects the evidence and makes an arbitration in case of disputes. Thus, it is inevitable to incur delay in the reputation update process. However, it is more important to make sure that the reputation management is transparent and is able to objectively reflect the trustworthiness of messages. Moreover, it is acceptable to update the reputation score after several hours in the specific scenario of VANETs. In this section, we will elaborate the reputation management of BARS in detail.

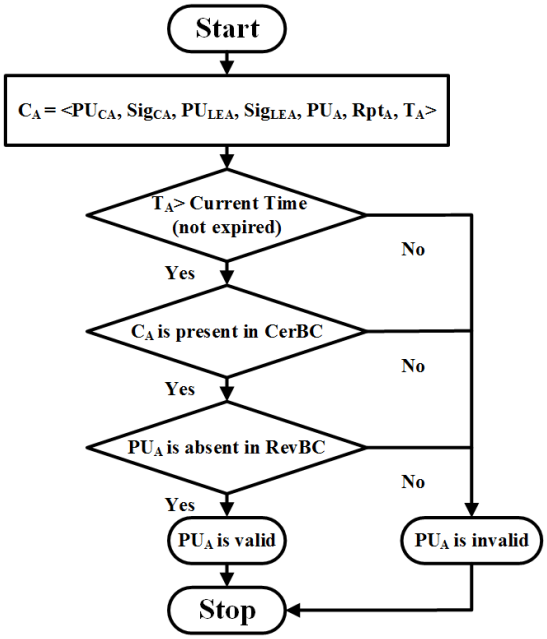


FIGURE 6. Privacy-preserving authentication process.

A. DIFFERENT TYPES OF MESSAGES

There are three types of messages: the beacon messages, the alert messages, and the exposure messages. Periodically, vehicles broadcast the beacon messages containing driving

status for the traffic management. The alert messages will be broadcasted when an emergency happens such as hard braking or losing control. If any vehicle disputes the authenticity of the received messages or discovers misbehaviors, they can send the exposure messages to LEA. Next, LEA will make an arbitration and the result will affect the reputation scores of the related vehicles. According to the criticality of emergency, the alert messages have three levels.

Level 1: When vehicle A loses control, it will automatically broadcast the alert messages with level 1 to avoid collision.

Level 2: The alert messages with level 2 are used for forewarning nearby vehicles before the sender changes its driving status, including braking, lane changing, etc.

Level 3: In case of poor road conditions such as obstruction or road damage, passing vehicles will broadcast the alert messages with level 3 to alert vehicles behind to keep caution.

B. REPUTATION EVALUATION ALGORITHM

The reputation evaluation algorithm consists of a reward mechanism and a punishment mechanism. There are two kinds of behaviors will be rewarded. First, vehicle A broadcasts alter messages honestly and actively. Second, vehicle A sends exposure messages to LEA when A discovers misbehaviors or receives forged messages. On the contrary, there are also two kinds of behaviors will be punished. First, vehicle A is exposed for misbehaviors or broadcasting forged messages. Second, vehicle A abuses exposure messages to slander other vehicles.

Intuitively, the criticality of an alert message, the sequence of senders, and the number of receivers should be taken into consideration in the reputation evaluation algorithm. Therefore, there are several factors affecting the reward mechanism and the punishment mechanism as follows:

L: The level of alert messages, L = 1, 2, 3.

D_r: The relative density of vehicles, $D_r = D/D_{aver}$. In this paper, D_{aver} is set to 20 vehicles per Km.

S: The sequence of the senders, S = 0, 1, …, n. S of the first vehicle to broadcast the alert message will be set to 0.

In addition, we set a reward coefficient α and a punishment coefficient β in the formulas to implement the reward mechanism and the punishment mechanism as follows.

$$R(L, S, D_r) = \alpha \cdot D_r \cdot \frac{1}{e^s \cdot L}$$

$$P(L, S, D_r) = (-1) \cdot \beta \cdot D_r \cdot \frac{1}{e^s \cdot L}$$

As explained in Algorithm 1, if no receiver disputes the authenticity of an alert message, the reputation scores of the senders will increase base on the reward mechanism (line 3). On the contrary, if any receiver sends exposure messages to dispute the authenticity of an alert message, LEA will collect evidence to make an arbitration. The vehicles who broadcast forged alert messages will be punished severely (line 15) while the vehicles who expose malicious behaviors will be rewarded (line 18). On the contrary, the vehicles who abuse exposure messages will also get punished (line 11) while the vehicles who broadcast authentic messages will be rewarded (line 8).

Algorithm 1 Reputation Evaluation Algorithm

Require: M_A: Alert message broadcasted by vehicle $V_i (i = 1, 2...n)$; M_D: Disclosure message broadcasted by vehicle $V_j (j = 0, 1...m)$; R'_i, R'_j: Current reputation score of V_i and V_j; S_i, S_j: The sequence of the senders; D_r: The relative traffic density.

Ensure: R_i, R_j: Updated reputation of V_i and V_j.

1: **if** $j = 0$ **then**
2: **for** each V_i **do**
3: $R_i \leftarrow R'_i + (100 - R'_i) \cdot \mathrm{R}(M_A.L, S_i, D_r)$
4: **end for**
5: **else**
6: **if** M_A is authentic **then**
7: **for** each V_i **do**
8: $R_i \leftarrow R'_i + (100 - R'_i) \cdot \mathrm{R}(M_A.L, S_i, D_r)$
9: **end for**
10: **for** each V_j **do**
11: $R_j \leftarrow R'_j + 25 \cdot \mathrm{P}(M_A.L, S_j, D_r)$
12: **end for**
13: **else**
14: **for** each V_i **do**
15: $R_i \leftarrow R'_i \cdot (1 + \mathrm{P}(M_A.L, S_j, D_r))$
16: **end for**
17: **for** each V_j **do**
18: $R_j \leftarrow R'_j + 50 \cdot \mathrm{R}(M_A.L, S_j, D_r)$
19: **end for**
20: **end if**
21: **end if**
22: **return** R_i, R_j

C. REPUTATION UPDATE

Vehicle A's reputation score is contained in the certificate and will be updated when a new certificate is issued to A. In this way, the reputation score is associated with a public key that acts as a pseudonym in V2V and V2I communications. If A's reputation score decreases to zero before the next update, A's public keys will be revoked immediately. Since the block generation time of CerBC and RevBC can be set to several minutes as Bitcoin and the proofs of presence and absence allow the receivers efficiently get the status of a public key, a vehicle with a bad reputation cannot continue to broadcast forged messages after a new block is generated.

VI. RESULTS AND ANALYSIS

In this section, BARS is evaluated in three aspects. First, we theoretically explain how BARS uses the extended blockchain technology and the cryptographic algorithms of PKI to achieve transparency, conditional anonymity, and robustness. Second, a specific scenario is simulated to illustrate how the reputation evaluation algorithm objectively reflects the trustworthiness of messages. Third, we implement

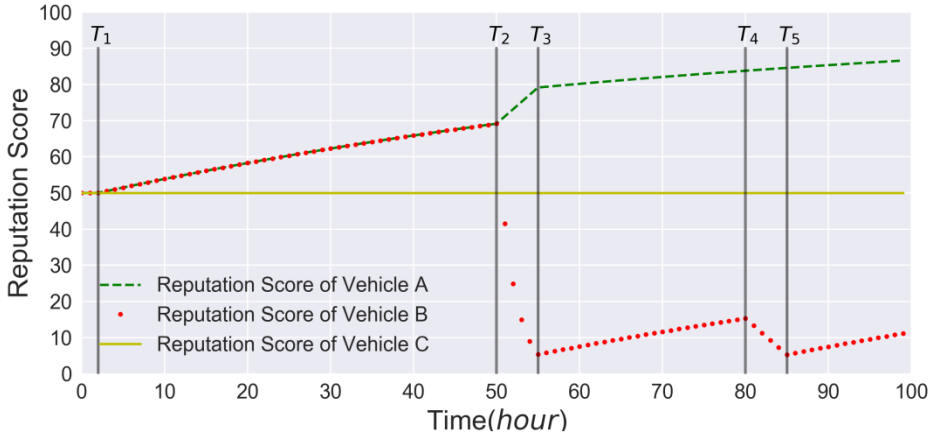


FIGURE 7. Reputation score of three vehicles.

BARS to evaluate the performance of each vehicle in the anonymous authentication under the assumption that authorities and RSUs have high enough computing power to support the operations of BARS.

A. SECURITY ANALYSIS

1) TRANSPARENCY OF AUTHORITIES

As explained before, CA and LEA are necessary for VANETs. The motivation of BARS is to make the activities of authorities transparent but not to eliminate them from VANETs. Each certificate transaction with its issued certificate and each revocation transaction with its revoked public key are recorded permanently in CerBC and RevBC respectively. Moreover, a transaction contains the timestamp and the digital signatures of CA and LEA. It means that all the entities in BARS are able to verify the transactions and figure out what CA and LEA have done.

2) CONDITIONAL ANONYMITY

Vehicle A uses public keys as pseudonyms for V2V and V2I communications without any information about its real identity. For the trade-off between security and privacy, the pairs of identities and public keys are stored with high-security level in LEA. It means that only LEA knows the real identity of any public key so that only LEA is able to track the malicious vehicle when it performs misbehaviors or broadcasts forged messages. A vehicle can get several certificates in a single request and change its public key at particular locations to enhance its privacy.

3) ROBUSTNESS OF BARS

Any change will eventually propagate to the root of the Merkle tree that is stored in the blockchain and cannot be tampered [27]. This nature of blockchain satisfies the robustness requirement of BARS. RSUs are responsible for verifying the transactions of CA and LEA and writing them into CerBC and RevBC respectively. PoW is provided by vehicles as the global consensus to guarantee that each entity has the identical public ledger, which consists of the authenticated certificates and the revoked public keys. Thus, CerBC and RevBC are unforgeable and immutable as long as more than half of vehicles in the network have not been compromised. The proof of presence in CerBC and the proof of absence in RevBC provide efficient authentication of the public keys of vehicle A. Then, vehicle A will use its private key to generate a signature for each broadcasted message and receivers can use A's public key to verify the signature. RSUs and vehicles cooperatively record all the broadcasted messages into the chronological MesBC, which is the persistent evidence in case of disputes.

B. VALIDITY OF REPUTATION EVALUATION ALGORITHM

In order to verify the validity of the reputation evaluation algorithm, we consider a scenario in which three vehicles perform different behaviors in 100 hours. As Fig. 7 illustrates, from T_1 to T_2 and T_3 to T_4, vehicle A and B broadcast safety messages to share information with other vehicles actively and honestly. Thus, their reputation scores increase gradually. From T_2 to T_3, vehicle B broadcasts five forged messages and is exposed by A. As a result, B gets published and B's reputation score decreases sharply whereas A gets rewarded and A's reputation score increases. From T_4 to T_5, vehicle B abuses five exposure messages to slander other vehicles, which causes B's reputation score to decrease. Vehicle C refuses to participate in BARS, C's reputation score remains unchanged at the initial value. The results show that all the behaviors of a vehicle in VANETs can be reflected objectively in its reputation scores.

C. PERFORMANCE EVALUATION OF ANONYMOUS AUTHENTICATION

We implement BARS in the Python environment using a laptop with 2.5 GHz Intel Core i5 and 8 GB 1600 MHz DDR3. Each vehicle is a miner equipped with a general-purpose computer and receives data from RSUs through V2I communication for the anonymous authentication.

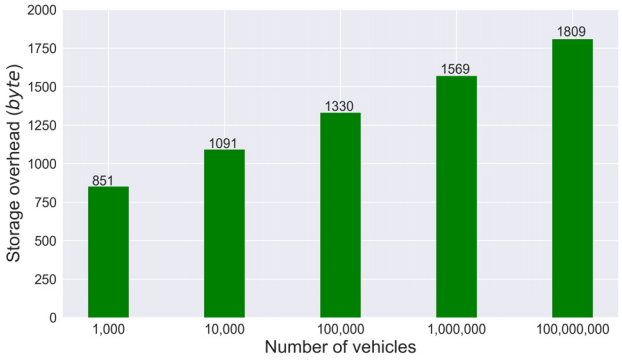


FIGURE 8. Storage overhead of the anonymous authentication.

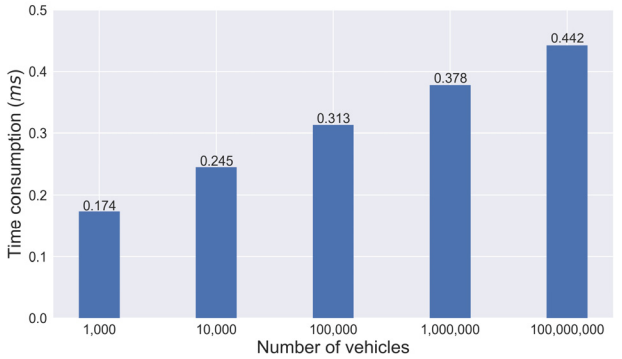


FIGURE 9. Time consumption of the anonymous authentication.

In V2V communication, the sender provides the data that is used to verify its public key based on the proof of presence in CerBC and the proof of absence in RevBC.

1) STORAGE OVERHEAD

A block header is about 80 bytes [8]. Suppose that new blocks are generated every 10 minutes, the storage overhead for one blockchain is 80 bytes $*$ 6 $*$ 24 $*$ 365 $=$ 4.2 MB per year. The data for the anonymous authentication consists of the associated certificate (about 100 bytes), the tuple for the proof of presence in CerBC, and the tuple for the proof of absence in RevBC. Suppose that there are a total of Num vehicles in the network, the storage overhead for a vehicle is S $=$ 100 bytes $+$ 32 bytes $* \log_2^{\mathrm{n}} +$ (32 bytes $+$ 8 bytes) $* \log_2^{\mathrm{m}}$, where n is the number of issued certificates and m is the number of revoked public keys. We assume that each vehicle has 5 unexpired public keys at the same time and 10% of all the public keys are revoked, i.e. n $=$ 5 $*$ Num, m $=$ 10% $*$ n. The storage overhead of the anonymous authentication for a vehicle in different scale VANETs is shown in Fig. 8.

2) TIME CONSUMPTION

The blockchains in BARS are built on SHA-256 whose time consumption is less than $\mathrm{t_1} = 0.01$ ms per 1 KB of input [28]. The proof of presence and the proof of absence are based on SHA-256 and can be done in time and space $\mathrm{O}(\log^{\mathrm{N}})$. Theoretically, the time consumption to authenticate one public key is $\mathrm{T} = \mathrm{t_1} * (\log_2^{\mathrm{n}} + \log_2^{\mathrm{m}})$. The time consumption of the anonymous authentication for one public key in different scale VANETs is shown in Fig. 9.

The storage overhead and time consumption of the anonymous authentication for a vehicle is accessible even in VANETs with 100,000,000 vehicles.

VII. CONCLUSION

In this paper, we address the issues of trust and privacy in VANETs. In order to prevent the distribution of forged messages from internal vehicles while simultaneously preserving the identity privacy of vehicles, a blockchain-based anonymous reputation system (BARS) is proposed for the trust management in VANETs. Two blockchains, CerBC and RevBC, make the activities of authorities transparent for all the entities in VANETs. The proofs of presence and absence provide the anonymous authentication with high efficiency. Public keys act as pseudonyms in V2I and V2V communications to preserve the identity privacy of vehicles. Moreover, all the broadcasted messages are recorded in MesBC as persistent evidence for evaluating each vehicle's reputation. A reputation evaluation algorithm is designed to prevent the distribution of forged messages and incent vehicles to expose misbehaviors. Finally, we analyze the security and validity of BARS and evaluate the performance of the anonymous authentication. The results show that BARS provides an effective trust model for VANETs with transparency, conditional anonymity, efficiency, and robustness.

REFERENCES

[1] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, 1st Quart., 2016.

[2] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, to be published.

[3] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[4] Y. C. Wei and Y. M. Chen, "Efficient self-organized trust management in location privacy enhanced VANETs," in *Proc. Int. Workshop Inf. Secur. Appl.* Berlin, Germany: Springer, 2012, pp. 328–344.

[5] B. Laurie, A. Langley, and E. Kasper, *Certificate Transparency*, document RFC 6962 (Experimental), Internet Engineering Task Force, 2013. [Online]. Available: http://tools.ietf.org/rfc/rfc6962.txt

[6] J. Yu, V. Cheval, and M. Ryan. (2014). "DTKI: A new formalized PKI with no trusted parties." [Online]. Available: https://arxiv.org/abs/1408.1023

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

[8] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

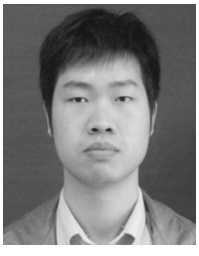
[9] M. Atzori, "Blockchain-based architectures for the Internet of Things: A survey," UCL–Res. Center Blockchain Technol., Tech. Rep., May 2016.

[10] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.

[11] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[12] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407–420, May 2011.

[13] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, 2012.
[14] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3657–3674, Aug. 2015.
[15] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. Int. Conf. Netw. Syst. Secur.* Berlin, Germany: Springer, 2013, pp. 94–108.
[16] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer Peer Netw. Appl.*, vol. 7, no. 3, pp. 229–242, 2014.
[17] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking," *Ad Hoc Sensor Wireless Netw.*, vol. 24, nos. 3–4, pp. 283–305, 2015.
[18] R. Hussain, W. Nawaz, J. Lee, J. Son, and J. T. Seo, "A hybrid trust management framework for vehicular social networks," in *Proc. Int. Conf. Comput. Social Netw.* Cham, Switzerland: Springer, 2016, pp. 214–225.
[19] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A categorized trust-based message reporting scheme for VANETs," in *Advances in Security of Information and Communication Networks*. Berlin, Germany: Springer, 2013, pp. 65–83.
[20] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.
[21] M. Al-Bassam, "SCPKI: A smart contract-based PKI and identity system," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, 2017, pp. 35–40.
[22] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Inf. Sci.*, vol. 462, pp. 262–277, Sep. 2018.
[23] A. Dorri, S. S. Kanhere, and R. Jurdak. (2016). "Blockchain in Internet of Things: Challenges and solutions." [Online]. Available: https://arxiv.org/abs/1608.05187
[24] Z. Lu, Q. Wang, G. Qu, and Z. Liu. (2018). "BARS: A blockchain-based anonymous reputation system for trust management in VANETs." https://arxiv.org/abs/1807.06159
[25] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent two-factor authentication," *IEEE Access*, vol. 6, pp. 32677–32686, 2018.
[26] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in VANETs," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 24, nos. 1–2, pp. 49–64, 2017.
[27] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ, USA: Princeton Univ. Press, 2016.
[28] S. J. Shackelford and S. Myers, "Block-by-block: Leveraging the power of blockchain technology to build trust and promote cyber peace," *Yale J. Law Technol.*, vol. 19, p. 334, Mar. 2017.



ZHAOJUN LU received the B.S. degree in electronic science and technology from the Huazhong University of Science and Technology, Wuhan, China, in 2013, where he is currently pursuing the Ph.D. degree in microelectronic and solid-state electronics. He is also a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park. His research interests include embedded system security, very large-scale integration design, and vehicular ad hoc network security.

WENCHAO LIU was born in Wuhan, China, in 1983. He is currently pursuing the Ph.D. degree with the School of Optical and Electronic Information, Huazhong University of Science and Technology. He is also a full-time Lab Staff with the School of Computer Science and Information Engineering, Hubei University, Wuhan. His main research areas include FPGA and hardware intrinsic security.

QIAN WANG received the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2014. She is currently pursuing the Ph.D. degree with the Maryland Embedded Systems and Hardware Security Laboratory, University of Maryland at College Park, College Park, USA. Her research interests include embedded systems, hardware security, and vehicular ad hoc network security.

GANG QU (SM'07) received the B.S. and M.S. degrees in mathematics from the University of Science and Technology of China, Hefei, China, in 1992 and 1994, respectively, and the Ph.D. degree in computer science from the University of California at Los Angeles, Los Angeles, CA, USA, in 2000. After graduation, he joined the University of Maryland at College Park, College Park, MD, USA, where he is currently a Professor with the Department of Electrical and Computer Engineering and the Institute for Systems Research. He is also the Director of the Maryland Embedded Systems and Hardware Security Laboratory, College Park, and the Wireless Sensors Laboratory. He is a member of the Maryland Cybersecurity Center and the Maryland Energy Research Center.

His primary research interests are in the areas of embedded systems and very large-scale integration (VLSI) computer-aided design (CAD) with a focus on low-power system design and hardware related security and trust. He studies optimization and combinatorial problems and applies his theoretical discovery to applications in VLSI CAD, wireless sensor networks, bioinformatics, and cybersecurity. He has received many awards for his academic achievements, teaching, and service to the research community. He serves as an Associate Editor for the IEEE EMBEDDED SYSTEM LETTERS, and the journal of *Integration*, and the *VLSI Journal*.

ZHENGLIN LIU received the Ph.D. degree from the Department of Electronic Science and Technology, Huazhong University of Science and Technology, Wuhan, China, in 2001.

He is currently a Professor with the School of Optical and Electronic Information, Huazhong University of Science and Technology. His main research interests include embedded system security and very large-scale integration design.