2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-being (IHSH) | 978-1-6654-4084-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/IHSH51661.2021.9378727

A Distributed Blockchain Based PKI (BCPKI) architecture to enhance privacy in VANET

Djilali MOUSSAOUI
Telecomunication dept.
University of Tlemcen
Tlemcen, Algeria
djilali.moussaoui@univ-tlemcen.dz

Benamar KADRI
Telecomunication dept.
University of Tlemcen
Tlemcen, Algeria
benamarkadri@yahoo.fr

Mohammed FEHAM
Telecomunication dept.
University of Tlemcen
Tlemcen, Algeria
mohammed.feham@univ-tlemcen.dz

Boucif AMMAR BENSABER *Computer science dept, UQTR university*
LAboratoire de Mathématiques et Informatique Appliquée
Trois Rivières, Canada
Boucif.Amar.Bensaber@uqtr.ca

***Abstract*—Among the important challenges for Vehicular Adhoc Network (VANET) Security and Privacy. Most of the solutions for privacy in vanet are based on pseudonyms. And the pseudonyms are digital certificates with very limited information, valid for a short time, and hide the identity of the vehicle. The pseudonym operations (issuing, changing, and revoking) are centralized by a certification authority. In our paper, we propose a fully distributed management for pseudonyms in VANETs. We use the blockchain technology to perform the different operations related to pseudonyms. Our proposal use two blockchains, one for registering pseudonyms, the second for revoked ones. The vehicles are considered as miners in the blockchain. Our approach makes the vehicles in VANET more autonomous in managing the security, and reduce the exchanged data with a centralized authority (Certificate Authority -CA)**

Keywords—privacy, vanet, blockchain, PKI

I. INTRODUCTION

Vehicle networks (VANETs) are fitted with wireless networking systems. Vehicles broadcast a variety of extremely classified information during conversations.
A malicious adversary can detect and pursue a car. This makes the security of vehicle privacy by anonymous authentication a key issue. Pseudonyms are important for avoiding illicit vehicle monitoring and maintaining anonymity in VANETs.
A variety of methods have been suggested to alter pseudonyms. These solutions, the centralized authority for controlling pseudonyms (emitting, revocation, changing), summarize the overall strategies used to guarantee anonymity in VANET by the authors[1]. In [2],[3] the authors talk about the distributed management of pseudonyms in VANET based on the blind signature.

Our proposition is based on blockchain technology, which is a fully distributed solution. The rest of this paper is structured as follows: a state of art in section II, the back round and relive concepts are presented in section III. The proposed system architecture is presented in section IV, and the security analysis is in section V.

II. THE STATE OF ART

A. Cryptographic based solutions in vanet

Cryptography provides the benefit of addressing and fixing several VANET security violations at once [4].

In [5], the authors used a distributed way based on asymmetric cryptography. A group key is used as parameters in a function *f*, $f(C_1,C_2,..,C_n)$, Ci is the contribution of the members, and either the group leader or a delegate can be the participant. The leader encrypts the contribution with each participant's public key and sends the prepared message to the participants of the group. Group participants have the option of determining the group key.

In[6], Busanelli et al. suggest a novel key control method for protected communications with VANET. They suggest a method for a sequence of short-lived secret keys to be created. The application targets V2V communications and consists of information being disseminated safely.

Steiner & al.[9] suggested an extension tailored for user groups called GDH (Group DH) in various variants based on the Diffie-Hellman key exchange method (GDH-1,GDH-2,GDH-3). CLIQUES is used in several proposed implementations for the sharing of collaborative keys. Steiner & al. suggest the protocol of IKA (Initial Key Agreement) to produce the original key.

III. BACKGROUND

The aim of this section is to provide the reader with the required context details and concepts, our proposed model is based on two concepts, the PKI system, and the blockchain technology.

A. The PKI system

The PKI guarantees the confidentiality of electronic transfers and the sharing of confidential information by means of cryptographic keys and certificates.

PKI provides security, access protection, integrity, authentication and non-repudiation services for e-commerce transactions and associated computer applications. The Certification Authority (CA), Registration Authority (RA), PKI Clients and Digital Certificates make up this scheme.

1) Certification Authority (CA)

The CA issues entities by issuing digital certificates, which is a digital document to create the entities' credentials to participate in a transaction. The digital certificate contains the entity's information (the name, the public key, validity period..). This data depends upon the arrangement of the company that issues the certificates [10].

2) Registration Authority (RA)

RA manage the interaction between the CAs and clients. In such situations, the RA shall serve as an agent between the CA and the customer. The tasks performed by the RA are set out below [10]:

- Receive substance demands and approve them
- Send the demands to the CA
- Receive the prepared certificate from the CA
- Send the certificate to the proper entity

A registration authority (RA) is an unit that is trusted by the CA to register [11].

3) PKI Clients

PKI clients are network entities that request a digital certificate from RA or CA. In order to receive a digital certificate from a CA, the customer must take the following steps: Submit a request to build a pair of keys (public and private). A request for the CA certificate is sent to the CA after the key pair is created [10].

4) Digital Certificates

A data integrity function is required to ensure that the modified public key is not undetected. Data integrity mechanisms alone are not adequate to ensure that the public key belongs to the claimed owner. A mechanism that links the key to a globally trusted party is required [10]. The two following aims should
be accomplished by the desired mechanism :

- Establishing the public key's integrity
- Link the public key and its related details to the owner in a trustworthy manner

B. blockchain technology

Blockchain infrastructure was initially developed to store financial transactions for the cryptocurrency of Bitcoin. It was the first protocol which resolved the problem of double spending. The challenge of stopping users of your scheme from spending a single digital token more than once is the double spending problem. Centered on cryptographically verifiable systems, the current state of the system is determined [12].

1) Consensus models

Nakamoto Consensus is an algorithm that determines which node should add a new block to the Proof of Work chain (PoW). In PoW, nodes called miners are attempting to solve a complicated cryptographic puzzle. The puzzle is designed in such a way as to make it impossible to solve, but easy to validate. This is called a cryptography trapdoor function [13].

C. Transactions

The transaction requires a header and a list of transactions. Each block header includes a Merkle root, a nonce, and a difficulty integer. Miners change values like a nonce to the point that their block hash is recognized as a valid new block hash [14], the structure is detailed with "Fig. 1,2".

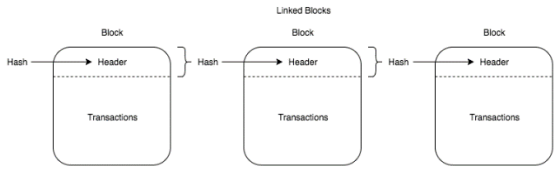

Fig. 1 Blockchain Structure

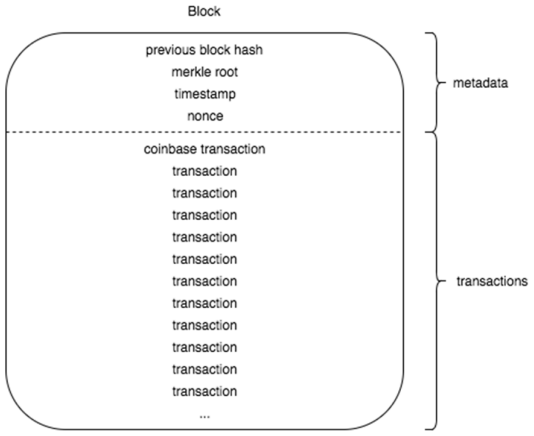

Fig. 2 Block structure

IV. SYSTEM ARCHITECTURE

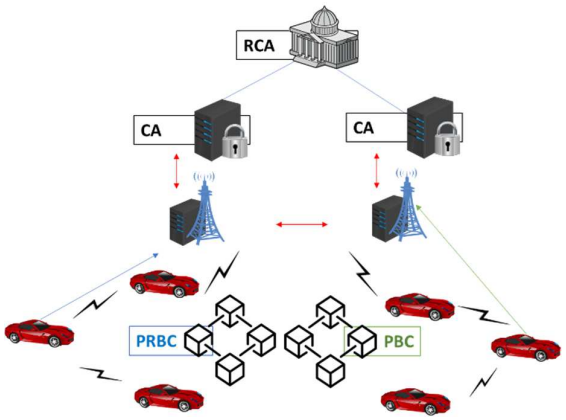

Fig. 3 BCPKI Architecture

A. COMPONENTS

1) RCA (Root Certificate Authority)

The RCA is the trust anchor in the scheme in which the trust is presumed and not derived, and its certificate is self-signed.
The key function is to issue and sign a certificate for the VCPKI security system's subordinate authorities only.

2) CA(Certificate Authority)

CA issue and sign a long-term certificate to the end-users (Vehicles). Each Vehicles must submit the request directly to the CA in order to receive a long-term certificate. In addition, the CA is able to issue tokens for vehicles that are used to demand PBC pseudonyms (short-term certificates) from the PBC (Pseudonym BlockChain).

3) RSU (Road-Side Unit)

The RSU is a wireless communication device, it is usually attached to the roadside or specific locations such as intersections or parking spaces.

4) PBC (Pseudonym BlockChain)

It is the blockchain where the pseudonyms are stored as a transaction, it acts as a public register for all the pseudonyms in the network**.** **"**Fig. 4" shows the structure of the PRBC.

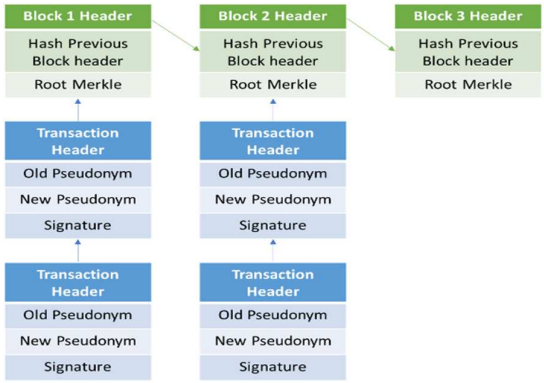

Fig. 4 Pseudonym BlockChain

The hash of the previous block header includes the block header and a root Merkle
The pseudonym transition is composed of the old pseudonym, the new pseudonym, and the digital signature of the pseudonym owner.

5) PRBC (Pseudonym Revocation BlockChain)

It is the blockchain to store the pseudonym revocation, the structure is detailed in "Fig. 5":

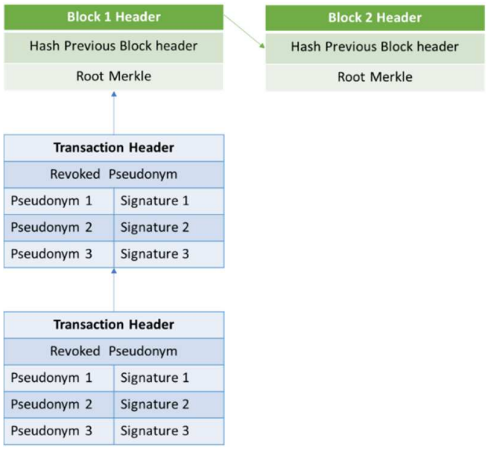

Fig. 5 Pseudonym Revocation BlockChain

The block header contains the hash of the previous header and root Merkle (Merkle root is the hash of the transactions hashes that forms a block).
The data stored in the transaction are the revoked pseudonym and three pseudonyms that ask for revoking pseudonym with their signature because the revocation is requested by the vote.

A. How it works

In this section, we will describe all the operations and exchanges.

1) Request for a long-term certificate(LTC):

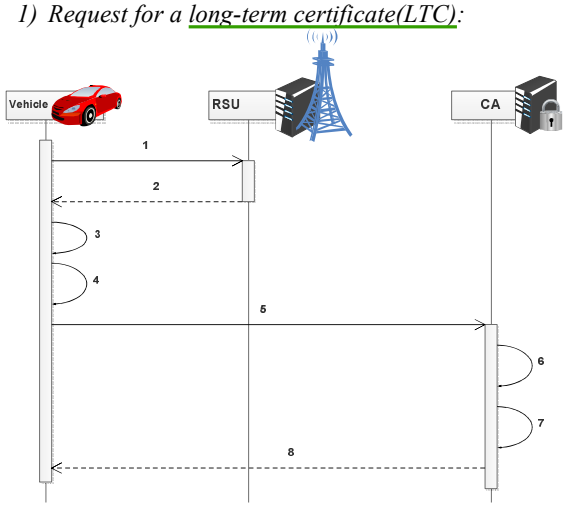

Fig. 6 Long Term Certificate Request

1. The vehicle requests the certificate from the RSU.
2. The RSU forwards the authority certificate (CA) to the vehicle.
3. The vehicle creates a key pair (public and private) with an elliptical curve.
4. The vehicle prepares a Certificate Signing Request (CSR), which is encrypted by the CA's public key.
5. The vehicle forwards a certificate request to the CA.
6. CA loads the private key to signs LTC and creates a certificate.
7. CA generates the initial pseudonym (initial Short-Term Certificate -iSTC)
8. CA returns the LTC and iSTC to the Subscriber.
9. CA stores the generated iSTC in the Pseudonym Blockchain (PBC).

2) Create a pseudonym (Short-Term Certificate STC)

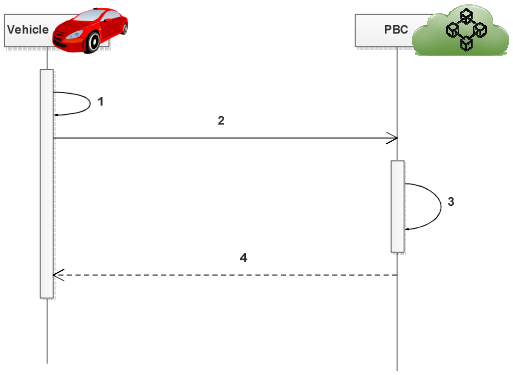

Fig. 7 Short Term Certificate (Pseudonym) Request

1. The vehicle creates a new pseudonym and defines its lifetime.
2. The vehicle sends the old pseudonym (initial pseudonym for first use -iSTC), the new pseudonym, and the lifetime as one transaction in the pseudonym blockchain (PBC).
3. Before validating the transaction, the old pseudonym has to verify two conditions:
- Registered in the Pseudonym BlockChain (PBC)
- Is not registered in the Pseudonym Revocation Chain (PRBC)
4. Vehicle receives a reply to its request (accept or reject)

3) Pseudonym revocation process

a) Revocation generation

1. If a V vehicle detects a node that misbehaves:

- V creates a Node Expulsion Message (NEM), which is a multi-signature message with V neighbors as signatories.
- V sends the NEM to the neighbors

2. If a Vn vehicle receives the NEM

- If Vn ∈ to the signatories of the NEM
- If the node has a bad behavior (stored in a local table)
  - Sign the NEM
  - If signatures ⩾ ½ of NEM signatories

- Create a Node Revocation Transaction Message (NRTM)

- Send the transaction to Pseudonym Revocation Blockchain (PRBC)

  - If not, transfer the NEM

- Otherwise, forward the NEM to other signatories.

b) Validation of the revocation transaction

Before the validation of the revocation operation, PRBC entities verify:

- If signature number ≥ ½

- If a signature ∈ PRBC then
  - Transaction rejected
- Otherwise, the transaction is validated.

4) Identity resolution

In the case where the identity must be revealed by the authorities (police), the process is as follows:

1. The authority identifies the pseudonym of the malicious node
2. The authority (the police) launches a request to search for the malicious node with its pseudonym
3. PBC searches for the initial pseudonym (generated by CA) in Pseudonym Blockchain by going back to the blockchain.
4. Once the pseudonym is found, PBC sends the initial pseudonym (generated by CA) to the Pseudonym Blockchain.
5. The authority (the police) generates a Real Identity Request-RIR (Real Identity Request-RIR)
6. Send the RIR to CA.
7. CA resolves the real identity

8. CA reviews the result to the authority (the police).

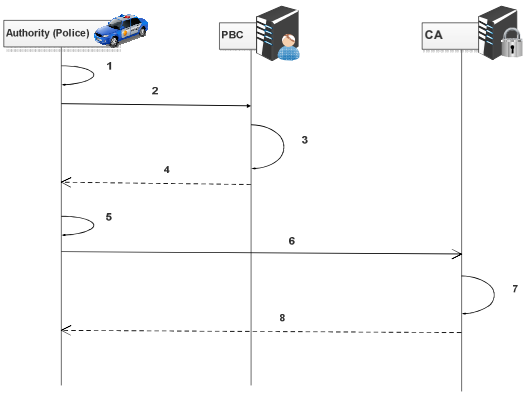

Fig. 8 Identity resolution

V. Security Analysis

The BCPKI is designed to enhance security especially privacy for vehicular networks. Our analysis will focus on the most affected [ref] requirements in vehicular cloud networks.

A. Integrity

This requirement is guaranteed by cryptography, since all exchanges in the PKI system are based on certificates (long term, short term) and public keys, all exchanges are encrypted, and the data is protected.

CA is the authority that manages the long-term certificates. Short-term certificates are managed by the PBC blockchain (Pseudonym Blockchain).

B. Privacy

To protect users' privacy, the temporary certificate or pseudonym is a very efficient tool.

In our case, we proposed decentralized management of pseudonyms using blockchain technology, that more very difficult to disclose the real identity of the pseudonym owner

C. Non-repudiation

The BCPKI is based on secure exchanges using various uses of asymmetric cryptography, and the digital signature is the way to guarantee non-repudiation, it is used either by the long-term certificate or by the short term certificate (pseudonym).

VI. Conclusion

In this paper, we suggest a fully distributed approach to manage pseudonyms. This approach is based on blockchain technology, where each node participates as a miner.

Our proposed solution enhances security by ensuring the security requirement for VANETs, especially privacy. The first pseudonym (initial pseudonym) is issued by the CA, and the vehicle generates a pseudonym, and ask for its registration in the blockchain by creating a blockchain transaction. We proposed two blockchains, the PBC(Pseudonym BlockChain) is used to store pseudonyms, and where a malicious node is detected, their neighbors create a revocation request, this request is signed by the neighbors, after verification, if the transaction is validated, the pseudonym is registered in the second Blockchain RPBC (Pseudonym Revocation BlockChain).

For future research, we will move to performance analysis and robustness against different attacks to validate our proposition.

References

[1] A. Boualouache, S. M. Senouci, and S. Moussaoui, “A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks,” IEEE Communications Surveys and Tutorials, vol. 20, no. 1, pp. 770–790, 2018.

[2] X. Zhu, Y. Lu, B. Zhang, and Z. Hou, “A distributed pseudonym management scheme in VANETs,” International Journal of Distributed Sensor Networks, vol. 2013, 2013.

[3] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, “Distributed Aggregate Privacy-Preserving Authentication in VANETs,” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, 2017.

[4] D. Moussaoui, M. Feham, B. A. Bensaber, and B. Kadri, “Securing vehicular cloud networks,” International Journal of Electrical and Computer Engineering (IJECE), vol. 9, no. 5, pp. 4154–4162, 2019.

[5] C. Boyd, “On key agreement and conference key agreement,” information Security and Privacy,Springer, pp. 294–302, 1997.

[6] S. Busanelli, G. Ferrari, and L. Veltri, “Short-lived Key Management for Secure Communications in VANETs,” in ITS Telecommunications (ITST), 2011, pp. 613–618.

[7] S. S. Kaushik., “Review of different approaches for privacy scheme in vanets,” International Journal of security and privacy, vol. 5, 2013.

[8] Josep Domingo-Ferrer and Qianhong Wu, “Safety and privacy in vehicular communications,” Privacy in Location-Based Applications, pp. 173–189, 2009.

[9] and G. T. Michael Steiner, Michael Waidner, “Cliques: A new approach to group key agreement,” in IEEE 33rd International Conference on Distributed Computing Systems, 1998.

[10] Y. Lee, J. Lee, and J. Song, “Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce,” Computer Communications, vol. 30, no. 4, pp. 893–903, 2007.

[11] D. R. Kuhn, V. C. Hu, W. T. Polk, and C. Shu-Jen, “SP 800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure,” National Institute of Standards and Technology, no. February, pp. 1–54, 2001.

[12] S. Nakamoto, ‘Bitcoin: A peer-to-peer electronic cash system,http://bitcoin.org/bitcoin.pdf,’ 2008.”

[13] A. Baliga, “Understanding blockchain consensus models,” 2017.

[14] X. Chen, “Blockchain challenges and opportunities : a survey Zibin Zheng and Shaoan Xie Hong-Ning Dai Huaimin Wang,” Int. J. Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.