Efficient Revocation and Anonymous Revocation in VANETs using Ring signatures

Maharage Nisansala Sevwandi Perera[1,a)] Toru Nakamura[1,2,b)]
Masayuki Hashimoto[1,c)] Hiroyuki Yokoyama[1,d)] Chen-Mou Cheng[1,4,e)]
Kouichi Sakurai[1,3,f)]

Abstract:
Vehicular Ad-hoc NETworks (VANETs), a special kind of Mobile Ad-hoc NETworks (MANETs), plays an important role in Intelligent Transportation Systems (ITS), allowing communication among vehicles and between vehicles and road-side units (RSUs). Among the performance requirements in VANETs, managing revocation of misbehaved vehicles took significant attention as it hindrances the practicability of VANETs. Even though numerous works proposed solutions for revocation management in VANET, there is no clear winner with secured and efficient revocation. This paper proposes two different solutions for revocation management for VANETs. The first solution presents efficient revocation, which does not require any authority involvement. The second proposal provides anonymous revocation, which guarantees the privacy of vehicles even though they are being revoked. Moreover, this paper presents extended privacy for revoking parties using ring signatures.

Keywords: VANET, revocation, efficient revocation, anonymous revocation, ring signatures

1. Introduction

Vehicle Ad-hoc NETworks (VANETs), one of the fundamental components of Intelligent Transportation Systems (ITSs), enables vehicles to exchange road conditions and their status via wireless communication systems. As a result, VANET ensures the safety and efficiency of transportation systems and provides comfort for drivers and passengers. Typically each vehicle is tailored with wireless On-Board Units (OBUs) to communicate messages with other vehicles and infrastructure (V2I). Road-Side Units (RSUs), set up along roads, act as Internet providing units and message propagators specifically distributing updated messages received from infrastructure services and supplying extra road-related information to vehicles.

Thus VANETs provides communications among V2V and V2I as shown in Figure 1.

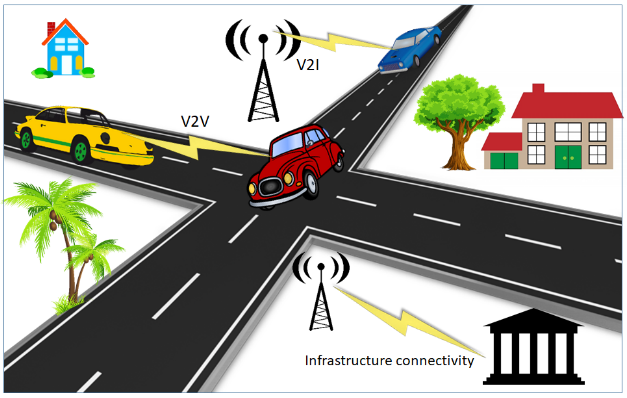

Fig. 1 VANET system

In these networks, authentication, confidentiality, privacy and anonymity, traceability and revocation of users (auditability), integrity, authenticity, undeniability, public verifiability, and linkability are necessary security requirements [1]. Since an eavesdropper can easily trace the communication pattern, the privacy of the vehicle (driver) is in danger. For instance, the driver's residence can be easily tracked down by observing the communication starting and ending of a vehicle. Thus, privacy, that is, the anonymity of vehicles, is desirable. However, since anonymity opens paths to crimes, linkability between messages to the vehicle is required to a certain level. Vehicles should be recognized when they misbehaved. Pseudonym schemes are widely used to enable user privacy and control their misbehaviors.

[1] Adaptive Communications Research Laboratories, Advanced Telecommunications Research Institute International (ATR), Kyoto, Japan
[2] KDDI Research, Inc., Saitama, Japan
[3] Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka, Japan
[4] Kanazawa University, Kanazawa, Japan
[a)] perera.nisansala@atr.jp
[b)] tr-nakamura@atr.jp
[c)] masayuki.hashimoto@atr.jp
[d)] hr-yokoyama@atr.jp
[e)] cheng@se.kanazawa-u.ac.jp
[f)] sakurai@inf.kyushu-u.ac.jp

When a vehicle with a unique id VID requests pseudonyms, the pseudonym issuing authority validates VID and issues pseudonym credentials to the vehicle. Since the maintenance of single pseudonyms is vulnerable to attacks, VANETs use a set of pseudonyms for each vehicle. Typically pseudonyms are assigned with an expiry date or validity period. Short validity periods and expiry dates ensure security against Sybil attacks. The message sending vehicle uses a valid pseudonym to authenticate himself as a valid user. However, The unlinkability property of pseudonyms prevents message receivers from understanding that these messages originated from a single node without performing additional plausibility checks, such as position verification [3]. Thus a mischievous vehicle may try to get advantages like clear the path ahead of him by providing fake messages. To prevent such kinds of forgeries, OBU requires fresh pseudonyms to authenticate a vehicle. Expired pseudonyms should not be used. Some approaches provide pre-loading of a large number of pseudonyms sufficient for few years, and some approaches provide refilling of pseudonyms periodically from the pseudonym issuer.

In traditional VANETs, if an RSU or a vehicle detects a misbehaving vehicle(s), it will report the incident to the centralized authority (CA), the pseudonym issuing authority. After confirming the misbehavior, CA will add all pseudonym certificates of the misbehaving vehicle to the certificate revocation list CRL.The pseudonym issuing party - CA may hold escrow information linking to pseudonym certificates that he provides. Thus CA gains the ability to revoke the anonymity of vehicles by linking pseudonyms to the VID of each vehicle. Periodically CA broadcasts CRL, and the message verifiers use updated CRL for authenticating a received message. The CA is solely responsible for revoking pseudonym certificates.

Centralized revocation involves considerable time delay due to reporting, investigation, updating CRL with thousands of misbehaving vehicles' certificates, and broadcasting of CRL. Until the updated CRL is broadcast, mischievous vehicles may continue their attacks. Thus, centralized revocation affects the safety of other vehicles. One of the solutions is decentralized revocation. In 2019, Bao et al. [4] presented a pseudonym management scheme from blockchain structure. In their proposal, the vehicle network structure is separated into blocks, and each block has a privacy manager PM who interacts with the centralized authority to update CRL. Since revoked pseudonym details are collected with the support of PMs, centralized revocation cost is reduced. However, until the CA gets information from PMs, misbehaving vehicles have a chance to continue their destructive actions. On the other hand, Asghar et al. [2] presented a voting-based decentralized revocation protocol, where a group of vehicles is capable of revoking a misbehaving or malicious vehicle within the communication range via a secure voting procedure. Asghar's [2] proposal prevents malicious vehicles from jeopardizing further by restricting them from sending or receive messages immediately. Thus comparing to the traditional VANETs, it ensures the safety of other vehicles as vehicles do not need to wait for CA's action. However, we observe that in such systems, a group of vehicles that are acquaintances may revoke a targeted vehicle. This may support hiding crimes. For instance, if a law enforcement party is in the middle of identifying the path of a criminal's vehicle, that vehicle may hide itself with the support of his coalition vehicles.

Thus we believe, revocation of suspicious vehicles should not be done permanently without the higher authority investigation. On the other hand, revocation should be done in minimum time for other vehicles' security. Answering these challenges, we present two proposals for pseudonym revocation.

1.1 Contribution

For both of our proposals we provide distributed framework for efficient revocation and authentication. We adopt the blockchain structure concept of Bao [4] and assign block manager BM for each block. Selected RSUs for each block can act as BMs for a particular block. The CA assigns these BMs, and they are provided with initial revocation and other information. Each BM is responsible for periodically updating CA with the latest local CRL (LCRL) and getting updated information from CA. To improve the revocation process, we allow vehicles (users) to revoke suspected or targeted vehicles in the vicinity (within the block) temporarily. On the other hand, we allow RSUs (BMs) to manage revocation based on the linkability of complaints it receives from vehicles for the exact targetted vehicle.

Thus, in this paper, first, we propose an efficient revocation with the support of Asghar's [2] proposal. Our proposal provides more efficiency on authentication as the message receivers must check the temporary CRL (TCRL) before the LCRL specific to the block. Periodically BMs gather temporary CRL (TCRL) and update CA with LCRL. The CA investigate the TCRL and update LCRL after confirming the validity of revocation details. On the other hand, as our second proposal, we allow BMs to execute revocation based on the linkability of the complaints received from vehicles in its block. We believe CA maintains mappings of VID, pseudonyms, and revoked information. Thus based on the LCRL received periodically, CA updates that mapping information. For instance, CA updates BMs according to the vehicle movement from one block to another with precise revocation details. Since our proposals provide a block-based structure for VANETs and local-wise revocation information, the verification cost of messages is also reduced. On the other hand, since both vehicles and BMs (RSUs) can execute revocation without waiting for CA's revocation process, it prevents further actions of mischievous or targeted vehicles. Moreover, in proposal one, where a group of users revokes a mischievous vehicle by voting, we ensure the privacy of those voting vehicles by adopting ring signatures. Thus, no mischievous or targeted vehicle can attack the voting vehicles later. However, we enable traceability of each vehicle and their action for CA. Thus, our proposals provide efficiency and anonymity for the revocation process.

2. Background and Related Works

With the development of VANETs, which provides V2V and V2I communication to ensure secured and safe driving, numerous research works were published. Moreover, several organizations like Preserve in Europe, IntelliDrive in the USA, and ITS in Japan have been established. VANETs technology should satisfy important security and privacy concerns [5], [6]. To prevent malicious users from abusing the system, vehicles and RSUs should authenticate receiving messages. On the other hand, the anonymity of vehicles should be satisfied to ensure their privacy. By employing digital signatures and signing the broadcasting messages, these security requirements can be accomplished. At the same time, misbehaved vehicles can be punished by revoking their certificates. Thus, message receiving vehicles trust only authenticated messages signed by non-revoked peers. However, peers (vehicles) should not have a long lifespan single certificate to prevent privacy issues. A potential solution is Security Credential Management System (SCMS) [7], [8], [9] which is one of the leading candidates in the USA. In the SCMS process, each vehicle carries multiple pseudonym certificates, which probably last longer for few years. Thus even though each pseudonym is short-lived, since the batch of certificates carried by each vehicle is sufficient for few years, vehicles do not require to refill certificates for a long time. On the other hand, since a message signed by an exact vehicle cannot be linked unless the same certificate is reused too often, the privacy of the vehicle is ensured. However, SCMS provides certificate revocation and linkage when misbehavior occurs. When malicious behavior is observed, centralized authority CA adds all the pseudonyms of that vehicle to the revocation list CRL.

One of the problems of the revocation process of traditional VANETs is the increase of CRL. Since one vehicle carries a batch of pseudonyms, CRL size increases when those certificates are added. Answering this CRL expansion problem, many works, including the efficiency of revocation using activation codes [10] and relying on Bloom Filters [11], [12] were proposed. Another problem is the effects of centralized revocation. In SCMS, the pseudonym certificate issuing authority CA retrains escrow information of each vehicle and pseudonyms to revoke later. Since CA is solely responsible for revoking pseudonyms, punishing misbehaved vehicles' revocation process is not efficient. As a result, until CA invokes the revocation process, mischievous users get the opportunity to harm the system further. Aiming to reduce the communication overhead and supporting CA to gather information of vehicles, Bao et al. [4] suggested a blockchain structure-based pseudonym certificate management scheme. As a solution to prevent jeopardize of identified vehicles, Asghar et al. [2] presented a voting-based scheme, where a group of users can revoke a vehicle by voting in their vicinity. Before Asghar's work some related work were proposed. Papadimitratos et al. [13] distributed CRL as small pieces in the network. Laber et al. [14] also employed V2V communication to distribute CRL in the network.

There are numerous research works addressing computation and communication cost of revocation of pseudonyms [2], [4], [13], [15], and the survey paper presented by Petit et al. [16] presented pseudonym schemes for VANET, including most of the revocation approaches. However, only a few approaches discussed the security and efficiency issues in centralized revocation [2], [11], [17]. Among them, even though Asghar et al. [2] suggested a voting-based system to prevent a user from compromising the system, they did not concern the issue that we focused on. We discuss the risk of hand overing the revocation ability to users other than security and efficiency challenges in centralized revocation. We decentralize the revocation process via block structure and ensure the security of the system and users.

3. Achieving Efficiency for Revocation and Authentication via User Voting

3.1 Blockchain Based Structure

Our proposals are based on the blockchain structure. Thus as in general-blockchain, centralized authority is removed, and public ledger, in our proposal the common CRL, is maintained. However, different from the general blockchain concept, we allow only centralized authority CA to update CRL. Other users can only read CRL. On the other hand, we maintain block-wise CRL (LCRL) for each block, which is connected with CRL and can be accessed by both CA and other users. The basic structure of the blockchain-based VANET system is depicted in Figure 2.

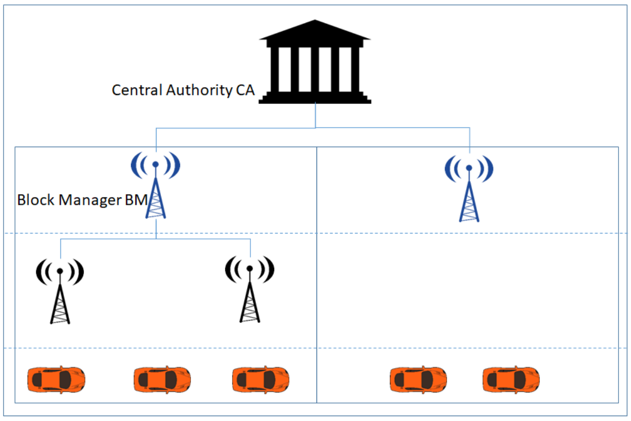

Fig. 2 Basic blockchain structure based VANET

Based on the hierarchy of responsibilities, the network consists of four layers. In the top layer, centralized authority CA is responsible for issuing certificates, revocation, and distributing CRL and other data. Moreover, CA assigns block managers (BMs) for each layer. Each BM is responsible for its logical coverage area. It interacts and supports CA to manage the network and maintains local CRL (LCRL) and revocation processes in his area. It is required to install

BMs in suitable geographical places. Vehicles communicate safety messages with other vehicles and RSUs. When a vehicle is registered with CA, CA provides a batch of pseudonym certificates and saves vehicle id VID and issued pseudonym certificates in a mapping table. Each certificate has its own expiring time. Thus, safety messages transmitted by vehicles include a pseudonym certificate, a timestamp, and the vehicle's current status. Vehicles are supposed to use each pseudonym for only a short period. Until CA updates revocation lists, each block gets revocation details of nearby blocks due to the blockchain structure.

In traditional VANET systems, CA investigates and updates CRL with the batch of pseudonym certificates of the culprit when misbehavior is found. In the proposing blockchain-based system, BMs and other users support revocation.

Once a vehicle i enters a new block, it interacts with BM by providing his pseudonym id PID_i. We believe each vehicle receives PID from CA at the registration process, and PID is for a batch of pseudonyms. BM checks CRL and LCRL and if the given PID_i is valid, he provides certificate for the block member ($BC_i = BlockId||PK_i$). Thus BC_i has a link to the block id. When transmitting a message, a vehicle should attach BC_i along with the pseudonym certificate. Thus message receiving vehicle authenticates that the message sending vehicle is in the same block. On the other hand, when a vehicle is misbehaved, BC_i is used to track and revoke the particular vehicle.

3.2 Voting based Revocation

We modify the above basic blockchain structure-based system to support voting-based revocation. In a voting-based revocation system, users in a block should be able to revoke a misbehaving vehicle. Since a group of users may revoke an innocent vehicle using this technique, we allow only temporary revocation from voting-based revocation. Thus each block has another revocation list TCRL other than the LCRL. Moreover, each BC_i has related secret key SK_i. Thus, when a vehicle registers to a block, the particular BM provides $BC_i = BlockId||PK_i$ a public key and $BCS_i = SK_i$ the corresponding secret key. When a vehicle transmits a message, it signs the message with secret key BCS_i and sends the message with BC_i and pseudonym. Thus a message receiver authenticates the message with given BC_i and pseudonym.

When a misbehaving vehicle is detected, a vehicle can execute a ballot to the targeted vehicle's BC_i, and other block users can vote. Once the threshold voting value k is achieved, that BC_i is added to $TCRL$ for a limited time t. Thus, the mischievous vehicle will be inactivated for t time or unless CA releases it (probably if it is innocent). Periodically BM collects TCRL information and updates CA along with LCRL and registered vehicle details in the block. If any vehicle is found guilty, then CA updates CRL and distributes new LCRLs for each block.

Since vehicles in a block can prevent malicious vehicles from jeopardizing the system further, the proposed system secures the other vehicles. On the other hand, since vehicles cannot permanently revoke a vehicle, innocent vehicles get active in the system after CA's decision.

3.3 Ensuring Participant Anonymity

Since voting is publicly available the targeted vehicle may track the voting parties and may attack later. To prevent such kind of attacks, we can ensure the privacy of voters by employing ring signatures. Ring signatures allow a user to be anonymous by employing an ad-hoc group. A user generates a ring signature including his and group of valid public keys.

In our proposal explained above, when a vehicle enters to a block it gets BC_i as his public key. By improving that method, here we say, the vehicle gets other existing vehicles public keys BC_n along with his BC_i. Thus when executing a voting, a user can generate a ring signature with selected public keys and his key to be anonymous.

We depict the anonymous voting based efficient revocation we proposed in above subsections in Figure 3.

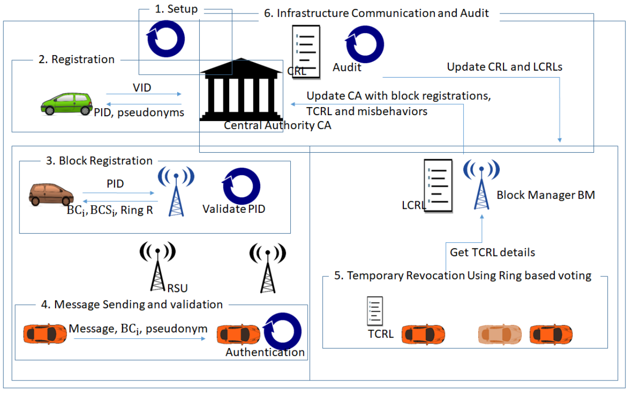

Fig. 3 Efficient and Safe revocation from ring based voting

Algorithms

(1) Setup: CA first partitions the network in to geographical blocks and assigns BMs for each block. CA initializes CRL and LCRLs, and broadcasts them. Moreover, CA decides other parameters like temporary revocation time, threshold votes, and block ids for each block.

(2) Registration: When a vehicle interacts CA with vehicle id VID, CA executes $\mathsf{KeyGen}(VID) \rightarrow (PID, pseudonyms)$ and returns (PID, pseudonyms) to the vehicle. CA maintains a mapping table of VID, PID, and pseudonyms.

(3) Block-Registration: When a vehicle enters to a block it interacts with the block manager with his PID. The block manager BM validates PID. First he checks in LCRL and then in CRL. After validation BM issues $BC = (BlockId||PK), BCS$, and the ring R by executing $\mathsf{BlockKeyGen}$(BlockId, PID). The ring R consists of other block users' BCs.

(4) Message Sending and validation: A vehicle transmits

a message M by signing with a valid pseudonym and appending BC and employed pseudonym. The message receiving party (another vehicle or RSU) authenticates the sender $\mathsf{Authenticate}$(M, BC, pseudonym, BlockId).

(5) Temporary Revocation Using Ring based voting: When a vehicle observes a mischievous vehicle, it executes a voting $\mathsf{RevokeVoting}(m = BC_w, BCS, R, t, k)$, where BC_w is the malicious vehicle's block certificate id, R is the ring, and t and k are time and threshold value of votes respectively. Here t and k are static values. Once number of votes reaches k the vehicle of BC_w is inactivated for t time. That is BC_w is added to the temporary revocation list TCRL. During t if BM collects and sends TCRL to CA, and CA decides the vehicle of BC_w is innocent, then the vehicle is activated.

(6) Infrastructure Communication and Audit: Periodically block managers BMs gathers TCRL details and sends to CA with other information of the block like current status of the block, new registrations of vehicles in the block, and LCRL. Then CA investigates, permanently revokes mischievous vehicles, and updates CRL and LCRLs accordingly.

4. Anonymous Revocation via Linkability

In the above provided proposal, a vehicle uses a valid pseudonym when transmitting a message. Another method is using ring signatures to sign a message. Employment of ring signatures improve the privacy of users.

When a new vehicle i registers with his VID, CA provides PID_i, pseudonyms, and a Ring R, where R consists of a set of valid PIDs. We assume a valid vehicle can get fresh R periodically. Thus when a vehicle enters to a block he generates a ring signature σ_j to join the block by using a valid ring R and a valid pseudonym. The block manager BM provides BC. Thus when transmitting a message a vehicle generate a signature with ring R (not R_b) and a valid pseudonym, and broadcasts the message attaching the BC. As a result, message receiving party can validate the message against the ring and confirm the block of the vehicle. In this proposal we enable BMs to revoke malicious vehicles. Here a vehicle or RSU or BM can link two signatures from same malicious users using the linkability of ring signatures [18]. On the other hand, BM can link malicious user with the signature generated at the block-registration. Thus BM can add malicious vehicle's block certificate to LCRL and updates local users and CA. Since CA can identify the vehicle using the mapping table he can confirm the revocation. In this proposal, BM could not identify vehicle because of the anonymity provided by ring signatures. Thus privacy of the vehicle is ensured even at the time of revocation.

Algorithms

(1) Setup: CA first partitions the network in to geographical blocks and assigns BMs for each block. CA initializes CRL and LCRLs, and broadcasts them.

(2) Registration: When a vehicle interacts CA with vehicle id VID, CA executes $\mathsf{KeyGen}(VID) \rightarrow (PID, pseudonyms)$ and returns (PID, pseudonyms, R) to the vehicle. CA maintains a mapping table of VID, PID, and pseudonyms. R is consists of valid vehicle PIDs. A vehicle can get valid R from CA periodically.

(3) Block-Registration: When a vehicle enters to a block it interacts with the block manager by generating a signature $\sigma_b \leftarrow \mathsf{blockJoin}(m_j, pseudonym, R)$. The block manager BM validates σ_b and issues $BC = (BlockId||PK), BCS$, and the ring R_b by executing $\mathsf{BlockKeyGen}$(BlockId, pseudonym). The ring R_b consists of other block users' BCs.

(4) Message Sending and validation: A vehicle transmits a message M by signing with a valid pseudonym and appending BC. The message receiving party (another vehicle or RSU) authenticate the sender $\mathsf{Authenticate}(M, R_b, BlockId)$.

(5) Local Revocation: When BM observes a malicious action he links the malicious signature with the signatures used for joining the block. If two linked signatures are found then updates LCRL and passes to CA.

(6) Infrastructure Communication and Audit: Periodically block managers BMs sends LCRL to CA with other information of the block like current status of the block, new registrations of vehicles in the block. Then CA updates CRL and distributes block information to blocks.

5. Conclusion and Future Work

In this paper we provided two proposals for efficient but unforgiable revocation and for anonymous revocation. Both schemes decentralizes the revocation process of existing VANET proposals. By employing ring signatures we ensure the privacy of vehicles. In future, we extend the provided preliminary ideas to a concrete scheme and analyze the efficiency and security with the existing schemes.

References

[1] Aghabagherloo, A., Mohajeri, J., Salmasizadeh, M., Feghhi, M. M. (2020, August). An Efficient Anonymous Authentication Scheme Using Registration List in VANETs. In 2020 28th Iranian Conference on Electrical Engineering (ICEE) (pp. 1-5). IEEE.

[2] Asghar, M., Pan, L., Doss, R. (2020). An efficient voting based decentralized revocation protocol for vehicular ad hoc networks. Digital Communications and Networks, 6(4), 422-432.

[3] Hubaux, J. P., Capkun, S., Luo, J. (2004). The security and privacy of smart vehicles. IEEE Security & Privacy, 2(3), 49-55.

[4] Bao, S., Lei, A., Cruickshank, H., Sun, Z., Asuquo, P., Hathal, W. (2019, August). A pseudonym certificate management scheme based on blockchain for internet of vehicles. In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 28-35). IEEE.

[5] Förster, D., Kargl, F., Löhr, H. (2014, December). PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). In 2014 IEEE Vehicular

Networking Conference (VNC) (pp. 25-32). IEEE.

[6] Schaub, F., Ma, Z., Kargl, F. (2009, August). Privacy requirements in vehicular communication systems. In 2009 International Conference on Computational Science and Engineering (Vol. 3, pp. 139-145). IEEE.

[7] Available at: https://www.campllc.org/security-credential-management-system-scms-proof-of-concept-poc-implementation/

[8] Whyte, W., Weimerskirch, A., Kumar, V., Hehn, T. (2013, December). A security credential management system for V2V communications. In 2013 IEEE Vehicular Networking Conference (pp. 1-8). IEEE.

[9] Kolleda, J., Frank, L., Andrews, S., Poling, T., Fitzpatrick, D., Marousek, J., Hamilton, B. A. (2018). National security credential management system (scms) deployment support: Scms baseline summary report.

[10] Simplicio Jr, M. A., Cominetti, E. L., Patil, H. K., Ricardini, J. E., Silva, M. V. M. (2019). ACPC: Efficient revocation of pseudonym certificates using activation codes. Ad Hoc Networks, 90, 101708.

[11] Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J. P. (2007). Eviction of misbehaving and faulty nodes in vehicular networks. IEEE Journal on Selected Areas in Communications, 25(8), 1557-1568.

[12] Haas, J. J., Hu, Y. C., Laberteaux, K. P. (2009, September). Design and analysis of a lightweight certificate revocation mechanism for VANET. In Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking (pp. 89-98).

[13] Papadimitratos, P., Mezzour, G., Hubaux, J. P. (2008, September). Certificate revocation list distribution in vehicular communication systems. In Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking (pp. 86-87).

[14] Laberteaux, K. P., Haas, J. J., Hu, Y. C. (2008, September). Security certificate revocation list distribution for VANET. In Proceedings of the fifth ACM international workshop on Vehicular Inter-NETworking (pp. 88-89).

[15] Wasef, A., Shen, X. (2011). EMAP: Expedite message authentication protocol for vehicular ad hoc networks. IEEE transactions on Mobile Computing, 12(1), 78-89.

[16] Petit, J., Schaub, F., Feiri, M., Kargl, F. (2014). Pseudonym schemes in vehicular networks: A survey. IEEE communications surveys & tutorials, 17(1), 228-255.

[17] Wasef, A., Shen, X. (2009). EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 58(9), 5214-5224.

[18] Torres, W. A. A., Steinfeld, R., Sakzad, A., Liu, J. K., Kuchta, V., Bhattacharjee, N., Cheng, J. (2018, July). Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1. 0). In Australasian Conference on Information Security and Privacy (pp. 558-576). Springer, Cham.